Fault-Tolerant Quantum Computation on Logical Cluster States(Dissertation_全文)

AUTHOR(S):

Fujii, Keisuke

Fault-Tolerant Quantum Computation on Logical Cluster States

Keisuke Fujii

2010

Contents

Chapter 1

Introduction

Recently, remarkable experimental progress has been made in various quantum systems such as linear optics, cavity QED, ion traps, optical lattices, and quantum dot arrays. It enable us to manipulate quantum states and employ them for a certain kind of information tasks, namely *quantum information processing* [1].

In 1982, Richard Feynman pointed out that a simulation of quantum systems on classical computers is generally inefficient due to the exponentially increasing dimension of the state space with the number of particles [2]. Instead, quantum systems should be simulated by other quantum systems efficiently. David Deutsch put this idea forward by formulating a quantum version of a Turing machine, which is a first precise model of an universal quantum computer [3]. Quantum computer has a great deal of potential, enabling us to solve some sorts of problems, which are thought to be intractable with classical computers. A great progress was made by Peter Shor in 1994 who demonstrated that large numbers can be factorized efficiently, i.e., within polynomial time by using quantum computer [4, 5]. Since factorization is exponentially inefficient for classical computers (so-called nondeterministic polynomial time (NP) problem, which means finding a solution is exponentially inefficient, but an answer can be verified efficiently), it is used for RSA (Rivest-Shamir-Adleman) encryption. It is, for instance, used to send credit-card numbers in Web browsing software. The Shor's discovery, which breaks the RSA encryption, has a great impact and triggered in leading quantum computer from a mere "Gedankenexperiment" to a physical device. On the other hand, in 1984, Charles Bennett and Gilles Brassard proposed a quantum cryptography, so-called BB84, which makes use of quantum uncertainty principle [6]. The security is protected by the nature of quantum physics, the no-cloning theorem (one cannot clone quantum states without

any disturbance) [7].

As seen above, quantum information processing seems to be promising, providing fast and secure information processing. However, Rolf Landauer criticized by saying that all papers on quantum computing should carry a footnote: "This proposal, like all proposals for quantum computation, relies on speculative technology, does not in its current form take into account all possible sources of noise, unreliability and manufacturing error, and probably will not work." [8]. Actually, quantum coherence, which is an essential property in quantum systems, is quite fragile against noise due to interaction with the environment, i.e., *decoherence*, (this is why quantumness rarely appears in our daily life [9]). Since quantum states cannot be cloned [7], straightforward redundancy techniques do not work. Moreover, a Hilbert space is a continuous space, and this implies that it may be difficult to distinguish errors. Thus in order for quantum information processing to work, we have to develop novel ways to counteract the decoherence problem.

A first and big step was made by Peter Shor in 1995. He proposed a quantum error correction (QEC) code, which protects quantum information in quantum memory from decoherence [10, 11]. The QEC code encodes logical quantum information by using many physical quantum systems. Even if the physical qubits are affected by noise, the original quantum state can be recovered by using the redundancy. This idea is extended to protect quantum computation under imperfect gate operations, namely *fault-tolerant quantum computation* [11, 12]. The main achievement in the theory of fault-tolerant quantum computation is the threshold theorem; if the amount of noise per gate is smaller than a certain value, namely *the noise threshold*, quantum computation can be performed to arbitrary accuracy with a polynomial overhead [13, 14, 15, 16, 17, 18]. The noise thresholds have been calculated to be about $10^{-4} - 10^{-2}$ for a variety of fault-tolerant schemes based on concatenated QEC codes [19, 20, 21, 22, 23, 24, 25, 26]. Among them, the Knill's $C4/C6$ error-correcting architecture provides a very high noise threshold $\sim$ a few %, which has been a benchmark of experimental success. However, it still remains unclear whether one can achieve a higher noise threshold or not, and the resources usage can be reduced or not.

In this thesis we investigate a fault-tolerant scheme which works well even with a high error rate $> 1\%$ under reasonable resources usage. Specifically, we investigate fault-tolerant one-way quantum computation on verified logical cluster states. We can reduce the effective measurement error in one-way computation by replacing each physical qubit

with a logical one. It is, however, not a trivial task to prepare such large entangled states as cluster states of logical qubits with high fidelity. Thus, the main aim of this thesis is to develop a scalable way to construct logical cluster states with high fidelity. To this end, we divide whole cluster states into some fundamental clusters of finite size. The fundamental clusters are construct with postselection via a verification process, say *double verification*, which is specifically designed to achieve high fidelity. The verified states have not only high fidelity, but also a good error distribution, i.e., independent and identical for each physical qubit, namely *homogeneous* [27]. This property is quite useful to calculate the noise threshold easily. The verified fundamental clusters are connected to construct a cluster state required for a desired computation. Then, one-way computation is implemented fault-tolerantly by measuring the logical qubits. Since, in one-way computation, gate operations are represented by specific type of entangled states, the verification process prior to the computation can be viewed as *preselection* or *error-precorrection*. This enable us a reliable computation even with realistically noisy gate operations.

This thesis is based on the studies in Refs. [25], [26], [28], [29], [30]. The remaining parts of the thesis are presented as follows.

Chapter 2 is devoted to a review of key ingredients in fault-tolerant quantum computation. We preliminary introduce fundamental concepts in quantum computation such as universal quantum computation, stabilizer formalism, and measurement-based computation. The stabilizer formalism can elegantly describe a certain type of quantum states, so-called *stabilizer states*, including cluster states and quantum error correction codes. The measurement-based quantum computation (or one-way quantum computation, cluster model) is a universal model, where arbitrary quantum computation can be implemented via quantum teleportation by single qubit measurements. Next we mention how quantum decoherence due to interaction with environment can be modeled. Then we introduce quantum error correction codes, which can protect quantum information from quantum decoherence by virtue of redundancy. Further ingredients are required for *fault-tolerant quantum computation*, where the gate operations for error correction are noisy themselves. Finally we mention two important approaches for fault-tolerant quantum computation, *topological quantum computation* and *postselected computation*.

In Chapter 3, we present a detailed description of an architecture for fault-tolerant quantum computation, which is based on the cluster model of logical qubits. In this cluster-based architecture, concatenated computation is implemented in a quite differ-

ent way from the usual circuit-based architecture where physical gates are recursively replaced by logical gates with error-correction gadgets. Instead, some relevant cluster states, say fundamental clusters, are recursively constructed through verification and postselection in advance for the higher-level one-way computation, which namely provides error-precorrection of gate operations. The performance is analyzed with respect to the noise threshold and resources usage, by comparison with other fault-tolerant schemes.

In Chapter 4, the gadget for verification, namely *double verification*, developed in Chapter 3 is applied for entanglement purification – *entanglement purification with double selection*. The performance is analyzed with respect to the achievable fidelity of purified states and noise threshold of imperfection in local operations. We further discuss on general grounds how some of the errors which are introduced by local operations are left as intrinsically undetectable. The undetectable errors place a general upper bound on the purification fidelity. Then we show that the double selection is a simple method to remove all the detectable errors in the first order so that the upper bound on the fidelity is achieved in the low noise regime. The double selection is further applied to purification of multi-partite entanglement such as two-colorable graph states.

In Chapter 5, we try another construction of fault-tolerant one-way computation on verified logical cluster states. Specifically, we adopt a topological means for reliable fault-tolerance at the higher level (logical level) to achieve high performance. The finite size fundamental clusters, say *star clusters*, are constructed with the double verification. They are connected near-deterministically to form a three-dimensional (3D) cluster state for topological one-way computation. Finally, the topological one-way computation is implemented by measuring logical qubits in the 3D cluster state. Similarly to the cluster-based architecture in Chapter 3, the performance is analyzed with respect to the noise threshold and resources usage.

Chapter 6 is devoted to summary and conclusions.

Chapter 2

Quantum computation and fault-tolerance

In this Chapter, we review key ingredients in fault-tolerant quantum computation. In Sec. 2.1, we preliminarily introduce fundamental concepts in quantum computation, including universal quantum computation, stabilizer formalism, measurement-based quantum computation (or one-way quantum computation, cluster model). In Sec. 2.2, we introduce quantum error correction codes, which can protect quantum information from quantum decoherence by virtue of the redundancy. Then, further ingredients are required for quantum error correction to work fault-tolerantly. Finally we mention two important concepts, topological quantum computation and postselected computation, which are both of importance to understand the contents in the subsequent Chapters.

2.1 Quantum computation

2.1.1 Universal quantum computation

In classical information science, the minimum unit of information is described by a binary digit or *bit*, which takes a value either 0 or 1. Its quantum counterpart is a quantum bit, so-called *qubit*, which is a superposition of two orthogonal quantum states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.1}$$

where α and β are arbitrary complex values satisfying $|\alpha|^2+|\beta|^2 = 1$. Significant difference between a classical bit and a qubit is really lies in the above superposition. There are a lot of candidates for the two orthogonal states, for example, polarization of photon, spin-1/2 particle, electronic states of atoms, and so on.

Since time evolutions are given by unitary operators in quantum physics, gate operations for a single qubit can be given by 2×2 unitary matrices. Among them, the most fundamental gate operations are expressed by Pauli matrices:

$$X = \sigma_x = \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \sigma_y = \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \sigma_z = \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.2)$$

For later convenience, we define $I = \sigma_I = \sigma_0$ as the 2×2 identity operator. These X, Y, Z and $-iI$ generate a group, so-called *Pauli group*. In stead of $\{|0\rangle, |1\rangle\}$, we may also chose different orthogonal bases:

$$\{|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}\}, \quad (2.3)$$

or

$$\{|+i\rangle \equiv (|0\rangle + i|1\rangle)/\sqrt{2}, |-i\rangle \equiv (|0\rangle - i|1\rangle)/\sqrt{2}\}. \quad (2.4)$$

The unitary operator which transforms $\{|0\rangle, |1\rangle\}$ to $\{|+\rangle, |-\rangle\}$ is given by

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (2.5)$$

which is called *Hadamard operator*. Similarly, one can transform $\{|+\rangle, |-\rangle\}$ to $\{|+i\rangle, |-i\rangle\}$ by using the so-called *Phase operator*

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}. \quad (2.6)$$

These X,Y,Z,H and S are normalizers of the Pauli group (i.e., $U_C \sigma_i U_C^\dagger = \sigma_j$), and generate a group of single-qubit *Clifford operations* U_C. Since the single-qubit Clifford group is a discrete group, one cannot generate arbitrary single-qubit unitary operations. Fortunately, it is known that one can generate arbitrary single-qubit unitary operations with polynomial resources by addition of a non-Clifford operation [31, 32, 33]. For example, we can chose the so-called $\pi/8$-gate

$$U_{\pi/8} = e^{-i\pi Z/8} = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix} = e^{-i\phi} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \quad (2.7)$$

where ϕ is a certain phase.

For arbitrary n-qubit unitary operations, at least one two-qubit gate operation is inevitable. There are two famous two-qubit gates, so-called *controlled-Not* (CNOT) and *controlled-Z* (CZ) gates:

$$U_{\rm CNOT} = |0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes X_t, \quad (2.8)$$

$$U_{CZ} = |0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes Z_t, \quad (2.9)$$

where the subscriptions c and t indicate the control and target systems, respectively. It is known that any unitary operation can be constructed from these elementary gates $\{H, S, U_{\pi/8}, U_{\rm CNOT}\}$ or $\{H, S, U_{\pi/8}, U_{CZ}\}$ [31, 32, 33]. Such a set of elementary unitary gates is called a *universal set*.

2.1.2 Stabilizer formalism

One of the most important properties of quantum states is *entanglement*, which originates from nonlocality of quantum physics. A quantum (pure) state is entangled if and only if it cannot be expressed as a product state such as $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots |\psi_n\rangle$. Popular examples of entangled states are EPR (Einstein-Podolsky-Rosen) [34] and GHZ (Greenberger-Horne-Zeilinger) states [35]:

$$|\mathrm{EPR}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}, \tag{2.10}$$

$$|\mathrm{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}, \tag{2.11}$$

where $|ijk\rangle$ means $|i\rangle \otimes |j\rangle \otimes |k\rangle$. Although these examples are very simple, n-qubit entangled states are generally complicated, and it is exhausting to write down them explicitly.

An elegant way, so-called *stabilizer formalism*, is developed by Daniel Gottesman to describe a certain class of quantum states simply [36]. An n-qubit stabilizer state $|\psi\rangle$ is defined by

$$S|\psi\rangle = |\psi\rangle \quad \text{for all } S \in \mathcal{S}, \tag{2.12}$$

where $\mathcal{S}$ is an Abelian (commutative) subgroup, so-called *stabilizer group*, of the n-qubit Pauli group $\{-iI, X, Y, Z\}^{\otimes n}$. For example, the stabilizer groups of EPR and GHZ states are given by

$$\mathcal{S}_{\rm EPR} = \langle X \otimes X, Z \otimes Z \rangle, \tag{2.13}$$

$$\mathcal{S}_{\rm GHZ} = \langle X \otimes X \otimes X, Z \otimes Z \otimes I, I \otimes Z \otimes Z \rangle, \tag{2.14}$$

respectively, where $\langle \{S_i\} \rangle$ means a group generated by the generators $\{S_i\}$. As in the above case, if the number of the generators are equal to that of the qubits, the stabilizer state is a rank one state. One can also define subspaces by using stabilizers as follows:

$$\mathcal{S}_{|00\rangle,|11\rangle} = \langle Z \otimes Z \rangle, \tag{2.15}$$

$$\mathcal{S}_{|000\rangle,|111\rangle} = \langle Z \otimes Z \otimes I, I \otimes Z \otimes Z \rangle, \tag{2.16}$$

where the stabilizer subspaces are two-dimensional spaces spanned by $\{|00\rangle, |11\rangle\}$ and $\{|000\rangle, |111\rangle\}$, respectively.

As seen previously, the Clifford operations are normalizers of the Pauli group. This indicates that they map a stabilizer state to another stabilizer state:

$$\begin{aligned} U|\psi\rangle &= US_i|\psi\rangle & (2.17)\\ &= (US_iU^\dagger)U|\psi\rangle \equiv \tilde{S}_iU|\psi\rangle, & (2.18)\end{aligned}$$

where $\tilde{S}_i = US_iU^\dagger$ are the new stabilizer operators. Thus this class of operations can be described in the stabilizer formalism as maps of stabilizer operators. The commutation relations between the Clifford operations (H, CNOT, and CZ) and the Pauli operators are given as follows:

$$\begin{aligned} HXH &= Z, & (2.19)\\ HZH &= X, & (2.20)\\ U_{\rm CNOT}(X_c \otimes I_t)U_{\rm CNOT} &= X_c \otimes X_t, & (2.21)\\ U_{\rm CNOT}(I_c \otimes X_t)U_{\rm CNOT} &= I_c \otimes X_t, & (2.22)\\ U_{\rm CNOT}(Z_c \otimes I_t)U_{\rm CNOT} &= Z_c \otimes I_t, & (2.23)\\ U_{\rm CNOT}(I_c \otimes Z_t)U_{\rm CNOT} &= Z_c \otimes Z_t, & (2.24)\\ U_{CZ}(X_c \otimes I_t)U_{CZ} &= X_c \otimes Z_t, & (2.25)\\ U_{CZ}(I_c \otimes Z_t)U_{CZ} &= I_c \otimes Z_t, & (2.26)\\ U_{CZ}(Z_c \otimes I_t)U_{CZ} &= Z_c \otimes I_t, & (2.27)\\ U_{CZ}(I_c \otimes X_t)U_{CZ} &= Z_c \otimes X_t. & (2.28)\end{aligned}$$

These relations are very useful to understand error propagations in fault-tolerant theory, since they are specified by exchanging the orders between the Clifford gates and error operators (i.e., the Pauli operators).

2.1.3 Measurement-based quantum computation

In Deutsch's model of quantum computation (with some simplification), a quantum register is first prepared in some quantum state as the input. Subsequently, unitary gate operations are implemented on the input state, and the quantum output is generated. Finally the quantum output is read by measurements performed on the quantum register.

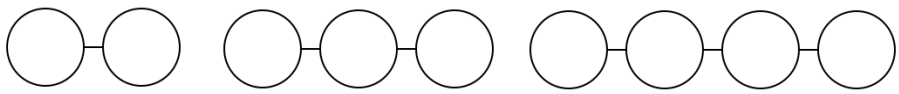
This quantum information processing analogous to the classical computation is called *quantum circuit model*. In the circuit model, unitary transformations are executed by deterministic unitary gate operations. Instead, one can also realize unitary transformations by using quantum teleportation, namely *quantum gate teleportation* [37, 38, 39, 40]. More precisely, the input state and a part of an entangled state are jointly measured (so-called Bell measurement), and the output state is generated with an unitary transformation via teleportation to the remaining quantum system. In 2001, Robert Raussendorf and Hans Briegel formulated a new model of quantum computation based on gate teleportation, namely *cluster model* (or *one-way computation*, or *measurement-based computation*) [41, 42, 43]. There, computation is executed by only single-qubit measurements on the resource states, namely *cluster states*.

Cluster states

A cluster state associated to a graph G is defined in terms of the stabilizer operators

$$K_j = X_j \bigotimes_{j'} Z_{j'}, \tag{2.29}$$

where the Pauli operators X_j and $Z_{j'}$ act on the qubits associated to the vertices j and j', respectively, and the tensor product is taken over all the vertices j' neighboring j [44, 43]. Cluster states are obtained systematically by preparing $|+\rangle^{\otimes n}$'s and performing CZ gates for the locations of the edges in the associated graphs. This can be understood from the facts that $|+\rangle$ is an eigenstate of the X operator, and that CZ gates transform X_j to K_j [see Eqs. (2.25)–(2.28)]. For example, two-, three-, and four-qubit cluster states, whose associated graphs are given by



(2.30)

are written explicitly as

$$|Cl_2\rangle = (|0\rangle|+\rangle + |1\rangle|-\rangle)/\sqrt{2}, \tag{2.31}$$

$$|Cl_3\rangle = (|+\rangle|0\rangle|+\rangle + |-\rangle|1\rangle|-\rangle)/\sqrt{3}, \tag{2.32}$$

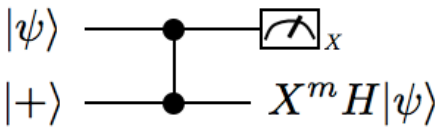
$$|Cl_4\rangle = (|0\rangle|+\rangle|0\rangle|+\rangle + |1\rangle|-\rangle|0\rangle|+\rangle + |0\rangle|-\rangle|1\rangle|-\rangle + |1\rangle|+\rangle|1\rangle|-\rangle)/\sqrt{4}, \tag{2.33}$$

respectively. The $|Cl_2\rangle$ and $|Cl_3\rangle$ are equivalent to the EPR and GHZ states up to local (single-qubit) Clifford operations, respectively. In general, an n-qubit stabilizer state is

equivalent to an n-qubit cluster state associated with a certain graph up to local Clifford operations [45, 46, 47].

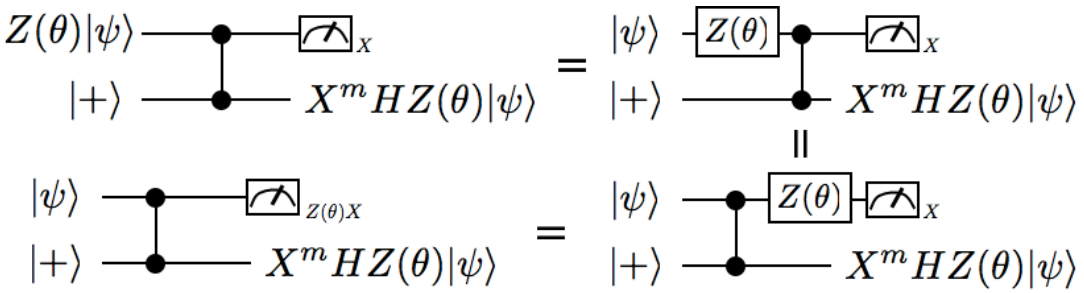
Single-qubit rotations

Next we consider how single-qubit measurements induce unitary operations via teleportation. Let us begin with the simplest case, where the input state $|\psi\rangle$ is connected with an ancilla state $|+\rangle$ via the CZ gate, then measured in the X basis $\{|+\rangle, |-\rangle\}$. The circuit diagram is given as follows:



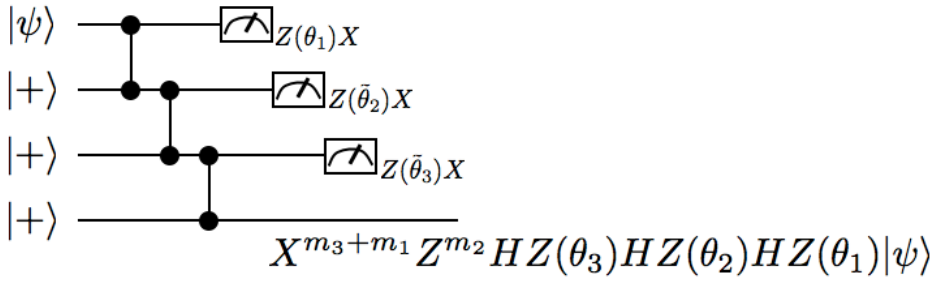
(2.34)

where m denotes the measurement outcome (i.e., classical one bit information 0 or 1). The input state is teleported with an Hadamard operation (up to a Pauli operator) to the output state, namely *one-bit teleportation*. By considering the following equivalences



(2.35)

one can understand that the $Z(\theta)XZ(\theta)^\dagger$ basis ($\{Z(\theta)|+\rangle, Z(\theta)|-\rangle\}$) measurement generates the output state, $X^m HZ(\theta)|\psi\rangle$, where $A(\theta) \equiv e^{-i\theta A}$. By combining one-bit teleportations with different angles, one can perform a sequence of single-qubit rotations as follows:



(2.36)

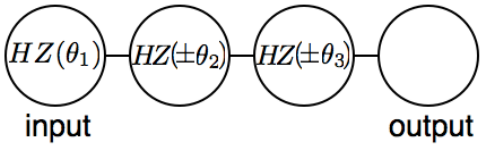
The output state is given as

$$
\begin{aligned}
&X^{m_1} HZ(\tilde{\theta}_3) X^{m_2} HZ(\tilde{\theta}_2) X^{m_3} HZ(\theta_1)|\psi\rangle \\
&= X^{m_3} HZ(\tilde{\theta}_3) X^{m_2} Z^{m_1} HZ((-1)^{m_1}\tilde{\theta}_2) HZ(\theta_1)|\psi\rangle \\
&= X^{m_3+m_1} Z^{m_2} HZ((-1)^{m_2}\tilde{\theta}_3) HZ((-1)^{m_1}\tilde{\theta}_2) HZ(\theta_1)|\psi\rangle, \qquad (2.37)
\end{aligned}
$$

where we have used a commutation relation $XZ(\theta)X = Z(-\theta)$. According to the measurement outcomes m_1 and m_2, the measurement bases are chosen adaptively as $\tilde{\theta}_2 = (-1)^{m_1}\theta_2$ $(= \pm\theta_2)$ and $\tilde{\theta}_3 = (-1)^{m_2}\theta_3$ $(= \pm\theta_3)$, respectively, to perform the operation

$$
HZ(\theta_3) HZ(\theta_2) HZ(\theta_1) = HZ(\theta_3) X(\theta_2) Z(\theta_1) \qquad (2.38)
$$

deterministically (up to Pauli operators) via teleportation. The above procedures are described in terms of the cluster diagram as follows [43]:

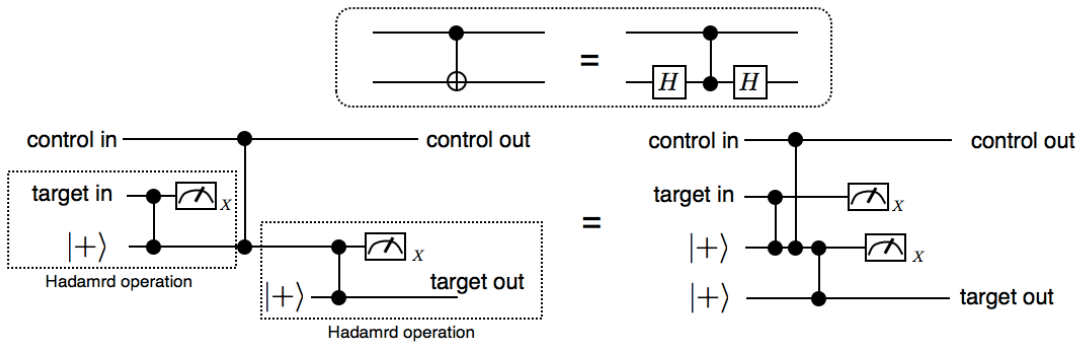


(2.39)

In general, one can describe any single-qubit rotation in the form of Eq. (2.38) by using the Euler decomposition. This shows that the above measurement-based computation can implement arbitrary single-qubit rotations.

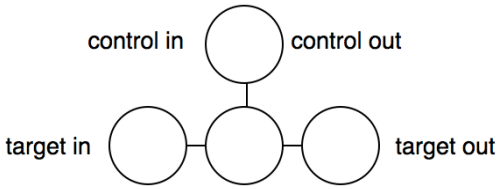
Two-qubit gates

One can also perform the CNOT gate ($U_{\rm CNOT} = I_c \otimes H_t U_{CZ} I_c \otimes H_t$) in one-way computation by considering the following equivalences



(2.40)

where the CZ gates are commutable with each other. Similarly to the single-qubit rotations, this is depicted in terms of the cluster diagram as follows:



(2.41)

Since the CNOT gate and single-qubit rotations compose a universal set, one can realize that an arbitrary unitary operation is implemented by combining the above two types of cluster states and measurements. Accordingly, the cluster states with single-qubit measurements provide a universal quantum computation model, say *cluster model*.

2.1.4 Linear optics and one-way computation

As seen so far, in the cluster model, any two-qubit gate operations are not required after preparing the cluster states. This property is quite useful for specific physical systems, where two-qubit gates are nondeterministic. In linear optics, for example, two-qubit gates are nondeterministic (probabilistic) due to the linearity of the interaction. In 2001, Emanuel Knill, Raymond Laflamme, and Gerard Milburn found that near-deterministic two-qubit gates can be realized by using teleportation, namely *KLM scheme* [48]. It, however, requires large ancilla states in the limit of unit success probability. In 2004, Michael Nielsen proposed to perform linear optical quantum computation deterministically by combining the KLM scheme with the one-way computation [49] (a related work [40] was also done before Ref. [49]). Subsequently, a resource efficient scheme was proposed based on the linear optical fusion gates, which succeed with 1/2 probability [50]. For general probabilistic two-qubit gates, possibly with much smaller success probabilities, efficient schemes have been discussed so far [51, 52, 53, 54, 55, 56, 57]. These works show that there are efficient schemes, whose total resources scale like polynomial in $1/p_s$, even if the success probability p_s is very small. Furthermore, fault-tolerance in the cluster model has been also discussed so far by considering clusterized versions of fault-tolerant schemes in the circuit model [58, 59, 60, 61, 62, 63].

2.2 Quantum error correction and fault-tolerant quantum computation

2.2.1 Quantum decoherence

In order to implement reliable computation in physical systems, either classical or quantum, the problem of noise should be overcome. Especially, quantum coherence, which is one of the essential properties of quantum systems, is quite fragile against noise due to interaction between the system and environment.

Under the Born-Markov (with rotating-wave) approximation, the time evolution of a two-level system coupled with an environment is given by a master equation of Lindblad form [64]:

$$\begin{aligned}\dot{\rho}(t) &= -\frac{\gamma_+}{2}\left[\sigma_-\sigma_+\rho(t) + \rho(t)\sigma_-\sigma_+ - 2\sigma_+\rho(t)\sigma_-\right] \\ &\quad -\frac{\gamma_-}{2}\left[\sigma_+\sigma_-\rho(t) + \rho(t)\sigma_+\sigma_- - 2\sigma_-\rho(t)\sigma_+\right] \\ &\quad -\frac{\gamma_0}{2}\left[\sigma_z\rho(t) + \rho(t)\sigma_z - 2\sigma_z\rho(t)\sigma_z\right] \equiv \mathcal{L}\rho(t), \end{aligned} \tag{2.42}$$

where $\sigma_+ = |0\rangle\langle 1|$ and $\sigma_- = |1\rangle\langle 0|$, and γ_α ($\alpha = 0, +, -$) are decay rates of the decay channels. One can easily find the eigenoperators of the Lindblad super-operator, which form the damping basis [65]:

$$\mathcal{L}\sigma_1 = \frac{\gamma_+ + \gamma_- + 2\gamma_0}{2}\sigma_1 \equiv \lambda_1\sigma_1, \tag{2.43}$$

$$\mathcal{L}\sigma_2 = \frac{\gamma_+ + \gamma_- + 2\gamma_0}{2}\sigma_2 \equiv \lambda_2\sigma_2, \tag{2.44}$$

$$\mathcal{L}\sigma_3 = (\gamma_+ + \gamma_-)\sigma_3 \equiv \lambda_3\sigma_3, \tag{2.45}$$

$$\mathcal{L}\rho_{eq} = 0, \tag{2.46}$$

where $\rho_{eq} = (\gamma_+|0\rangle\langle 0| + \gamma_-|1\rangle\langle 1|)/(\gamma_+ + \gamma_-) \equiv (\sigma_0 + a\sigma_3)/2$. The solution of this master equation can be given as a CP (complete positive) map $\mathcal{E}(t)$ [65]:

$$\mathcal{E}(t)\rho = p_0(t)\rho + \sum_{i=1,2,3} p_i(t)\sigma_i\rho\sigma_i + f(t)(\sigma_3\rho + \rho\sigma_3 - i\sigma_1\rho\sigma_2 + i\sigma_2\rho\sigma_1), \tag{2.47}$$

where

$$p_0(t) = \frac{1}{4}(1 + e^{-\lambda_1 t} + e^{-\lambda_2 t} + e^{-\lambda_3 t}), \qquad p_1(t) = \frac{1}{4}(1 + e^{-\lambda_1 t} - e^{-\lambda_2 t} - e^{-\lambda_3 t}), \tag{2.48}$$

$$p_2(t) = \frac{1}{4}(1 - e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-\lambda_3 t}), \qquad p_3(t) = \frac{1}{4}(1 - e^{-\lambda_1 t} - e^{-\lambda_2 t} + e^{-\lambda_3 t}), \tag{2.49}$$

$$f(t) = \frac{a}{4}(1 - e^{-\lambda_3 t}). \tag{2.50}$$

If we consider a high temperature case (i.e., $a \to 0$), Eq (2.47) can be rewritten as

$$\mathcal{E}(t)\rho = [1 - p_1(t) - p_2(t) - p_3(t)]\,\rho + \sum_{i=1}^{3} p_i(t)\sigma_i\rho\sigma_i. \tag{2.51}$$

Thus in the high temperature limit, the CP map of the noise can be viewed as stochastic Pauli errors with probabilities $p_i(t)$. In general cases, the noise cannot be written as Eq. (2.51). By performing relevant operations, however, one can depolarize the CP map to a standard form, i.e., stochastic Pauli errors in such a way that the noiseless part of the evolution is not altered [66]. Otherwise, Pauli basis measurements can collapse the CP map into stochastic Pauli errors, as shown later. In the following part of this thesis, therefore, we consider the Markovian stochastic Pauli noise such as Eq. (2.51). So far, fault-tolerance against more general noises has been discussed [17, 18, 21, 23, 24, 67]. If the decoherence is non-Markovian, dynamical decoupling or quantum Zeno effect can be used to suppress the decoherence [68, 69, 70, 71, 72, 73]. Besides, if the decoherence is spatially correlated, one can utilize a passive error-prevention scheme, so-called *decoherence free subspace* (DFS), which is immune to collective noise [74, 75, 76].

2.2.2 Quantum error correction codes

Three-qubit bit flip code

Quantum error correction (QEC) codes can be descried elegantly in the stabilizer formalism. Let us consider the simplest QEC code, three-qubit bit flip code, whose stabilizer generators are given by

$$S_1 = Z_1Z_2, \quad S_2 = Z_2Z_3, \tag{2.52}$$

where Z_i indicates the Pauli operator acting on the ith qubit. The stabilizer subspace is spanned by the following two logical states:

$$|0_L\rangle = |000\rangle, \quad |1_L\rangle = |111\rangle. \tag{2.53}$$

The logical Pauli-X operator is given by $X_1X_2X_3$. The logical Pauli-Z operator may be Z_1, Z_2, or Z_3, since the actions of these three operators are all the same for the code states. The logical Pauli-Y operator is given by the multiplication of the Pauli-X and Pauli-Z. This code is a quantum analogue of the classical three-bit repetition code. Consider a bit flip error with an error probability p:

$$\mathcal{E}_i\rho = (1-p)\rho + pX_i\rho X_i. \tag{2.54}$$

If the initial state $|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$ undergoes the bit flip error independently, the output state is transformed in the leading order as

$$\mathcal{E}_1 \circ \mathcal{E}_2 \circ \mathcal{E}_3 |\psi_L\rangle\langle\psi_L| = (1-p)^3 |\psi_L\rangle\langle\psi_L| + p(1-p)^2 \sum_i X_i |\psi_L\rangle\langle\psi_L| X_i + O(p^2). \quad (2.55)$$

Since the errors map the code space to the orthogonal spaces, the projective measurement onto the orthogonal subspaces, $P_k^{\pm} = (I \pm S_k)/2$, tells us what type of error most likely occurs. [Note that the projection operator of a Hermitian operator A, which has the eigenvalues ± 1, is given by $(I \pm A)/2$.] According to the measurement outcomes, the logical state can recover from the error as follows:

$$\mathcal{R} \circ \mathcal{E}_1 \circ \mathcal{E}_2 \circ \mathcal{E}_3 |\psi_L\rangle\langle\psi_L| = [(1-p)^3 + 3p(1-p)^2] |\psi_L\rangle\langle\psi_L| + O(p^2), \quad (2.56)$$

where the recovery operator is given by

$$\begin{aligned} \mathcal{R}\rho &= P_1^+ P_2^+ \rho P_2^+ P_1^+ + X_1 P_1^- P_2^+ \rho P_2^+ P_1^- X_1 + X_2 P_1^- P_2^- \rho P_2^- P_1^- X_2 \\ &\quad + X_3 P_1^+ P_2^- \rho P_2^- P_1^+ X_3. \end{aligned} \quad (2.57)$$

The four terms in $\mathcal{R}\rho$ correspond the measurement outcomes $(+,+)$, $(-,+)$, $(-,-)$, and $(+,-)$, respectively. By comparing Eqs. (2.55) and (2.56), one can understand that if p is sufficiently small, the fidelity of the logical state is improved.

Nine-qubit code

In the three-qubit case, one cannot correct Z errors, which are commutable with the stabilizers. The first QEC code, which can correct all X, Y and Z errors, was developed by Peter Shor in 1995. The stabilizer generators of the Shor nine-qubit code are given as follows:

$$\begin{array}{|ccccccccc|} \hline X & X & X & X & X & X & I & I & I \\ I & I & I & X & X & X & X & X & X \\ Z & Z & I & I & I & I & I & I & I \\ I & Z & Z & I & I & I & I & I & I \\ I & I & I & Z & Z & I & I & I & I \\ I & I & I & I & Z & Z & I & I & I \\ I & I & I & I & I & I & Z & Z & I \\ I & I & I & I & I & I & I & Z & Z \\ \hline \end{array} \quad (2.58)$$

The code space is spanned by

$$\frac{|0_L\rangle + |1_L\rangle}{\sqrt{2}} = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}, \quad (2.59)$$

$$\frac{|0_L\rangle - |1_L\rangle}{\sqrt{2}} = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}. \quad (2.60)$$

The logical Pauli operators are given by $X_L = X^{\otimes 9}$ and $Z_L = Z^{\otimes 9}$, which are bitwise tenser products of physical Pauli operators. Such a property, that is the logical A operator is given by a bitwise tenser products of physical A operators, is called *transversality*. The nine-qubit code is capable of correcting all X, Y and Z errors for each qubit, since they map the code space to different orthogonal spaces, so-called *syndrome spaces*.

Five-qubit code

The nine-qubit code is not the smallest QEC code which can correct all X, Y, and Z errors. The smallest code so far is the five-qubit code found by Ramond Laflamme *et al.* and Charles Bennett *et al.* independently [77, 78]. The stabilizer generators and logical Pauli operators are given as follows:

$$\begin{array}{rccccc} S_1 = & X & Z & Z & X & I \\ S_2 = & I & X & Z & Z & X \\ S_3 = & X & I & X & Z & Z \\ S_4 = & Z & X & I & X & Z \\ X_L = & X & X & X & X & X \\ Z_L = & Z & Z & Z & Z & Z \end{array} \tag{2.61}$$

The code states can be described simply by using the stabilizer operators:

$$|m_L\rangle \propto \prod_{k=1}^{4} \frac{I + S_k}{2} |m\rangle^{\otimes 5} \ (m = 0, 1), \tag{2.62}$$

where we have used the fact that $(I + S_k)/2$ are projections onto the code space. The five-qubit code is the smallest non-degenerate QEC code which satisfies the quantum Hamming bound:

$$\sum_{j=0}^{t} \left(\begin{array}{c} n \\ j \end{array} \right) 3^j \leqq \frac{2^n}{2^k}, \tag{2.63}$$

where t, n and k indicate the numbers of correctable errors, physical qubits and logical qubits, respectively (specifically, $t = 1$, $n = 5$ and $k = 1$ for the five-qubit code). The quantum Hamming bound means that the number of errors does not exceed that of syndrome spaces since different errors map the code space to different syndrome spaces (i.e., non-degenerate).

Seven-qubit code

In both cases of the five- and nine-qubit codes, the logical Pauli operators have transversality. However, other logical operations such as Hadamard and CNOT gates do not

have transversality in those codes. There is a class of QEC codes, so-called Caldrbank-Shor-Steane (CSS) codes, which have a high symmetry so that the logical CNOT gate has transversality [79, 80]. The smallest CSS code is the Steane seven-qubit code, whose stabilizer generators and logical Pauli operators are given by

$$\begin{array}{rcccccccc} S_1 & = & I & I & I & X & X & X & X \\ S_2 & = & I & X & X & I & I & X & X \\ S_3 & = & X & I & X & I & X & I & X \\ S_4 & = & I & I & I & Z & Z & Z & Z \\ S_5 & = & I & Z & Z & I & I & Z & Z \\ S_6 & = & Z & I & Z & I & Z & I & Z \\ X_L & = & X & X & X & X & X & X & X \\ Z_L & = & Z & Z & Z & Z & Z & Z & Z \end{array} \tag{2.64}$$

Similarly to the five-qubit case, the code states are described as

$$|m_L\rangle \ \propto \ \prod_{k=1}^{6} \frac{I+S_k}{2} |m\rangle^{\otimes 5} \ (m=0,1). \tag{2.65}$$

In the case of the CSS codes, different from the five-qubit code, the stabilizer generators can be written by using only X's and I's or Z's and I's. This implies the relationship between the CSS codes and the classical linear codes [79, 80]. Actually, the stabilizers of the seven-qubit code stem from the classical Hamming code. By virtue of this property, all CSS codes have transversality for the logical CNOT gate. This is because the transversal CNOT gate is a normalizer of the stabilizer group of two logical qubits $\langle \{I, S_k\} \otimes \{I, S_l\} \rangle$. Furthermore, note that in the case of the seven-qubit code, the X's in the generators S_1, S_2 and S_3 are replaced with the Z's in the generators S_4, S_5 and S_6. Such a symmetry is called *self-duality*. The self-dual CSS codes are invariant under the transversal Clifford operations. It ensures the trasversality of the logical Hadamard, Phase, CZ and CNOT gate operations.

Correcting all single-qubit errors

So far, we have described QEC codes which are capable of correcting all X, Y and Z errors. We here show that this is actually sufficient to correct all single-qubit errors. Consider a noise whose CP map is given in the Kraus representation,

$$\mathcal{E}\rho = \sum_i K_i \rho K_i^\dagger. \tag{2.66}$$

In general, the Karaus operators can be decomposed into Pauli operators as

$$K_i = \sum_j c_{ij}\sigma_j, \tag{2.67}$$

where $c_{ij} = \mathrm{Tr}[\sigma_j K_i]$. Since different Pauli errors map the code space to different syndrome spaces, the syndrome measurement $\mathcal{P}$ results in

$$\mathcal{P}\mathcal{E}\mathcal{P}\rho = \sum_{j=0}^{3} p_j \sigma_j \mathcal{P}\rho\sigma_j, \tag{2.68}$$

where $p_j = \sum_i |c_{ij}|^2$. Thus an arbitrary type of noise can be discretized by the syndrome measurement. Accordingly, the capability of correcting all X, Y and Z errors is sufficient to correct arbitrary single-qubit errors. This justifies the following analyses, where only the stochastic Pauli errors are considered.

Code distance

We finally mention an important quantity to measure the capability of a stabilizer QEC code, namely *code distance*. The distance of a stabilizer code is defined as the minimum number of X's or Z's in the operators which map the code state to itself acting non-trivially. The three QEC codes, we have considered so far, all have the distance three, and they are capable of correcting one error. In general, a QEC code of distance $d = 2n+1$ is able to correct n errors.

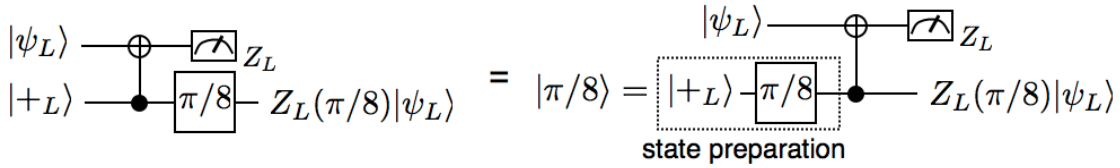
2.2.3 Fault-tolerant quantum computation

So far we have considered several QEC codes, which can correct arbitrary single-qubit errors. Further ingredients, however, are required to realize reliable quantum computation. In fact, if the logical operations or syndrome measurements propagate a single error as multiple errors, the QEC does not succeed. One must therefore be able to compute on the encoded states without any error spreading. Such a procedure is called *fault-tolerant*.

Fault-tolerant universal gates

The transversal gates are apparently fault-tolerant, since there is no interaction within the code block. This is why the seven-qubit code, where the logical Hadamard, Phase, CZ, and CNOT gates have transversality, is very useful for fault-tolerant computation.

Generally for the stabilizer codes, it is known that the logical Clifford gates can be constructed fault-tolerantly (although it is not so simple as for the seven-qubit code) [81]. As the Gottensman-Knill theorem asserts, however, quantum computation which consists of only the Clifford operations can be efficiently simulated by using classical computers [1, 81]. Thus we need to develop a way to implement a non-Clifford gate fault-tolerantly for universal computation. Fortunately, there is a relatively easy way to implement the logical $\pi/8$ gate $Z_L(\pi/8)$ by using one-bit teleportation as follows:



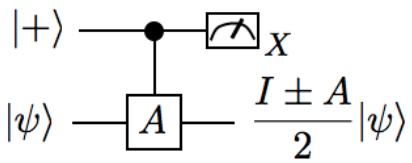
(2.69)

Note that the Z-basis measurement and CNOT gate are both transversal on the seven-qubit code. Thus, if the preparation of the non-Clifford ancilla state $|\pi/8\rangle = (|0_L\rangle + e^{-i\pi/4}|1_L\rangle)/\sqrt{2}$ is fault-tolerant, one can ensure fault-tolerance of the logical $\pi/8$ gate. A fault-tolerant preparation of the non-Clifford ancilla state has been developed by Sergey Bravyi and Alexei Kitaev, namely the *magic state distillation* [82]. There, the quantum Reed-Muller code, where a non-Clifford operation also has transversality, is used to distill the special ancilla state. This discovery has much simplified the construction of the fault-tolerant non-Clifford gate operation.

Fault-tolerant syndrome measurements

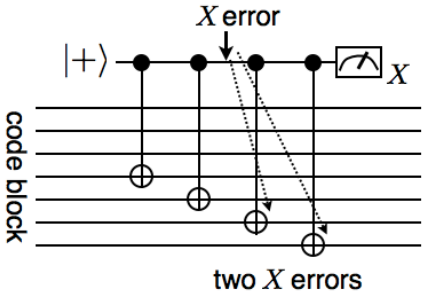
In the case of stabilizer code, the syndrome measurements are simply done by measuring the stabilizer operators. Several QEC gadgets have been proposed to implement the stabilizer measurement fault-tolerantly [12, 20, 83].

DiVincenzo-Shor's gadget— A QEC gadget was first proposed by David DiVincenzo and Peter Shor, where cat states are used as ancillae for the syndrome measurement [12]. It is based on an indirect measurement of the observable A with the eigenvalues ± 1:



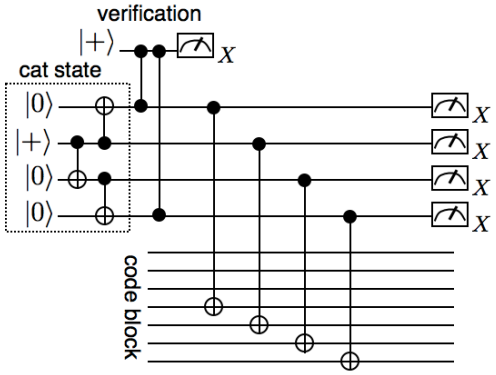
(2.70)

For example, the stabilizer S_1 of the seven-qubit code can be measured as the transversal X measurements of the corresponding physical qubits in the code block:



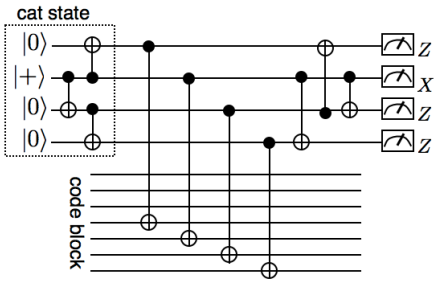
(2.71)

Unfortunately, this measurement is not fault tolerant, since the errors in the CNOT gates [$A = X$ in Eq. (2.70)] are spread by the following CNOT gates, as shown in the above circuit. To make it fault-tolerant, a cat state $|\text{cat}\rangle = (|000\cdots0\rangle + |111\cdots1\rangle)/\sqrt{2}$ is used as an ancilla for the measurement as follows:



(2.72)

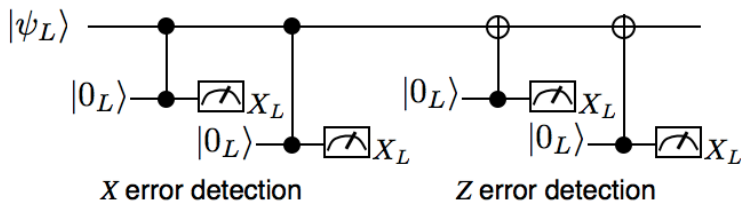
where the cat state is verified before connecting with the code state. Since the qubits in the code block interact with different ancilla qubits, this measurement does not spread the errors in the CNOT gates. Similarly, other stabilizers $S_2, \cdots, S_6$ are measured fault-tolerantly to obtain the error syndrome. Instead of the verification, one can perform a suitable recovery operation by postprocessing of the ancilla state after its interaction with the code state [84]:



(2.73)

The DiVincenzo-Shor's QEC gadget and its improved version both require a lot of physical gate operations, which results in deterioration of the performance.

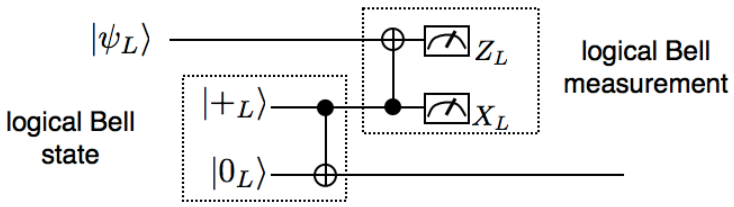
Steane's gadget— Subsequently, a relatively simple QEC gadget was proposed by Andrew Steane [83], where encoded ancilla states are used to extract the syndrome with transversal operations. In particular, for the case of CSS code, the logical code states can be used as ancilla states. The following circuit executes the Z and X error syndrome extractions by using the ancilla $|0_L\rangle$ states,



(2.74)

Since the ancilla states are the logical code states, one can obtain the error syndrome simply by measuring the ancilla states. The syndrome extraction is repeated for some times in order to extract the reliable error information. An optimized way to extract the syndrome information was proposed in Ref. [85], where the subsequent syndrome extraction is conditionally performed according to the preceding syndrome information. In order for these schemes to work fault-tolerantly, the encoded ancilla $|0_L\rangle$ states have to be prepared with high fidelity. This is achieved by using verification or entanglement purification [20, 83, 86, 87].

Knill's gadget— Another interesting QEC gadget was proposed by Emanuel Knill [20]. It is based on quantum teleportation as illustrated in the following circuit



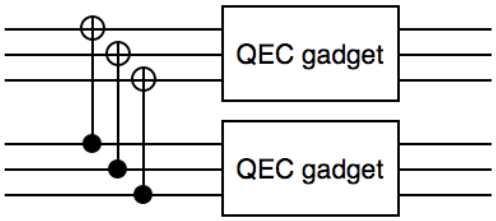
(2.75)

Here, the encoded data qubit $|\psi_L\rangle$ is teleported to the fresh encoded qubit of the ancilla Bell state. Thus the encoded ancilla Bell state has to be prepared with high fidelity by using verification or entanglement purification, similarly to the Steane's gadget. The outcome of the logical Bell measurement to complete the teleportation provides sufficiently the syndrome information, namely *error-correcting teleportation*. Thus, it is not necessary to repeat the syndrome extraction in this QEC gadget. The outcome of the Bell

measurement is properly propagated to the subsequent computation as the Pauli frame [20, 61, 62].

Fault-tolerant gate operations

Fault-tolerant computation is now executed by the logical gate operations which are followed by the QEC gadgets. This is illustrated for the fault-tolerant CNOT gate as follows:



(2.76)

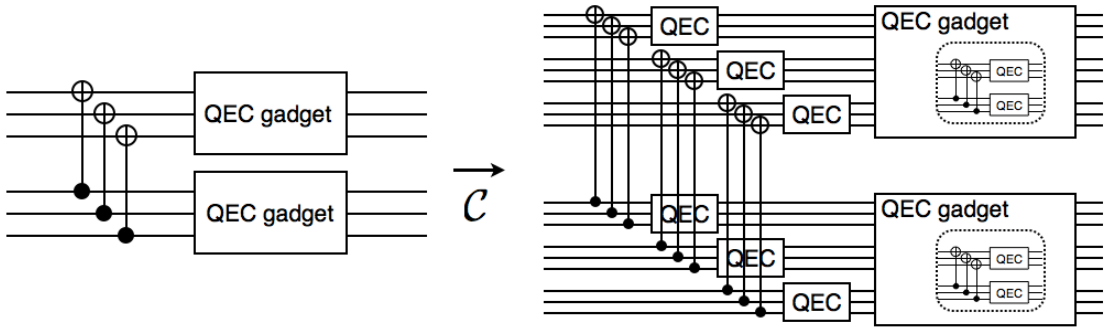
where the code block is depicted as though it is a three-qubit code. A QEC gadget is attached to each logical output of the transversal CNOT gate. Since a single error never be propagated as multiple errors in a fault-tolerant gate, a logical error is caused by two (or more) simultaneous physical errors. Denoting the number of such faulty pairs of error locations as C, the logical error probability is given by Cp^2, with p being the physical error probability. If the physical error probability is sufficiently small, $p < 1/C$, one can improve the accuracy of the gate to achieve fault-tolerant computation.

Concatenated quantum computation

For a reliable computation of a large size, the logical error probability should be reduced arbitrarily. This is done by concatenated fault-tolerant computation [15, 16, 17, 18]. In the concatenated computation, each physical gate operation is repeatedly replaced by a logical gate operation followed by QEC gadgets.

Suppose A is a quantum computation, which consists of some physical gate operations. Then the first level concatenated computation is defined by $\mathcal{C}(A)$, where the operation $\mathcal{C}$ indicates replacing each physical gate with a logical one followed by QEC gadgets. For example, $\mathcal{C}(\mathrm{CNOT})$ is described in the diagram (2.76). The second level concatenated

CNOT gate $\mathcal{C} \circ \mathcal{C}(\mathrm{CNOT})$ is also described as follows:



(2.77)

where each physical gate in the QEC gadgets is also replaced by the logical one followed by the QEC gadgets. By repeating this procedure, the lth level concatenated computation of A is given by $\mathcal{C}^l(A)$. Specifically, for a physical gate operation G (e.g., Hadamard, CNOT gate, and so on), we call $\mathcal{C}^l(G)$ as the level-l G gate. The lth level concatenated code state is called the level-l qubit, which is denoted as $|0^{(l)}\rangle$, $|+^{(l)}\rangle$.

As mentioned previously, the logical error probability $p_g^{(1)}$ of the level-1 gate is given by

$$p^{(1)} = C(p^{(0)})^2, \tag{2.78}$$

where $p^{(0)} = p$, and C denotes the number of all faulty pairs of error locations. The constant C is different among the logical gates. It is, however, sufficient to chose the maximum value. Due to the self-similarity of the concatenation, the logical error probability of the level-2 gate is given in terms of $p^{(1)}$ by

$$p^{(2)} = C(p^{(1)})^2. \tag{2.79}$$

Similarly, the logical error probability $p^{(l)}$ of the level-l gate is obtained recursively as

$$\begin{aligned} p^{(l)} &= C(p^{(l-1)})^2 \\ &= (Cp^{(0)})^{2^l}/C. \end{aligned} \tag{2.80}$$

This concludes that if $p^{(0)} < p_{\mathrm{th}} \equiv 1/C$, the logical error probability can be reduced super-exponentially with the concatenation level l. This is the so-called *threshold condition*.

On the other hand, resources usage $R^{(l)}$ consumed for the level-l gate is estimated roughly as

$$R^{(l)} = N^l, \tag{2.81}$$

where N indicates the total number of the physical gates in the level-1 gate. Suppose that the size of computation is $10^{n-1} = M$, then an accuracy $p^{(l)} < 10^{-n}$ is required for each logical gate at the highest level. Then the total resources to perform the reliable quantum computation of size M amount to

$$R_{\rm tot} \;=\; N^{\bar{l}} M = \left(\frac{n}{\log_{10}(Cp^{(0)})^{-1}} \right)^{\log_2 N} M = {\rm poly}(\log(M))M, \tag{2.82}$$

where $\bar{l} \simeq \log_2 \left[n / \log_{10}(Cp^{(0)}) \right]$ is the number of levels necessary to achieve the required accuracy. This result clearly shows that if the physical error probability $p^{(0)}$ is smaller than $p_{\rm th}$, one can execute quantum computation to arbitrary accuracy with only polylogarithmic overhead. This is the celebrated *threshold theorem*, and the critical value p_{th} is called the *noise threshold* [1, 13, 15, 16, 17].

The noise thresholds have been calculated to be about $10^{-4} - 10^{-2}$ for several fault-tolerant schemes under varying degrees of assumption and rigor [15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 88, 89].

The threshold values were first obtained at about the same time (1996) independently by Dorit Aharonov and Michael Ben-Or who used a polynomial code of distance five [17, 18], by Emanuel Knill, Raymond Laflamme and Wojciech Zurek who used the Steane seven-qubit code [15, 16], by Alexei Kitaev who used toric (surface) codes [13]. All of these works are based on concatenated computation mentioned above, and achieve similar threshold values $\sim 10^{-6}$. Subsequently the threshold values were improved to 10^{-5} independently by John Preskill and Andrew Steane [14, 88].

A great progress was made by Anderw Steane in 2003, who obtained numerically a high noise threshold $\sim 10^{-3}$ by using the Steane's QEC gadgets [19]. In 2005, Emanuel Knill obtained a considerably high noise threshold $\sim$ a few % by combining the Knill's QEC gadget with the Fibonacci scheme [20]. This work was a landmark, which increased the threshold value to about 1%, remarkably higher than the previous estimates.

On the other hand, in Refs. [21, 22, 23, 24] the noise thresholds (or lower bounds) were estimated in the rigorously proved way for the Steane seven-qubit code, four-qubit error-detection code, Bacon-Shor code, and Fibonacci scheme, respectively. They improved the rigorously proved thresholds from $10^{-6}-10^{-5}$ to $10^{-4}-10^{-3}$. There, however, still remains a large gap between the numerical and rigorous estimates of noise thresholds. These methods were also used with the Monte-Carlo simulation to compare the performances for a wide variety of the stabilizer QEC codes [89], which provides a comprehensive version

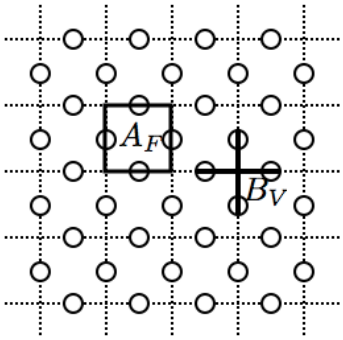


Figure 2.1: Square lattice to describe a surface code. Stabilizer operators A_F and B_V are associated with each face F and vertex V, respectively. A qubit is associated with each edge indicated with a circle.

of the previous work [19].

Recently a new approach was proposed to estimate the noise threshold with a relatively easy calculation. There, the error probabilities of logical ancilla states, which are used in the QEC gadgets, are assumed to be independent and identically distributed, namely *homogeneous* [27]. It, however, lacks an explicit way to construct such logical ancilla states scalably.

2.2.4 Topological quantum computation

We mention another remarkable approach toward fault-tolerance, which does not use the concatenated encoding. In 1997, Alexei Kitaev developed an important class of QEC codes, so-called *surface codes* [90, 91]. Subsequently fault-tolerant topological computation on the surface code was developed by Robert Raussendorf [92, 93, 94]. Consider an $N \times N$ square lattice, where a qubit is associated with each edge (see Fig. 2.1). The stabilizers of the surface code are defined associated with each face F and vertex V as

$$A_F = \bigotimes_{i \in F} Z_i, \quad B_V = \bigotimes_{i \in V} X_i, \tag{2.83}$$

where the tenser products are taken over the four qubits on the face and vertex, respectively. Apparently, the above A_F and B_V are commutable, and the surface code is one of the CSS codes. The numbers of stabilizer generators are L^2 and $(L+1)^2 - 1$ for A_F and B_V, respectively, where $\bigotimes_V B_V = I$ is considered. On the other hand, the number of qubits is $2L(L+1)$, which is equal to the total number of stabilizer generators. Thus the

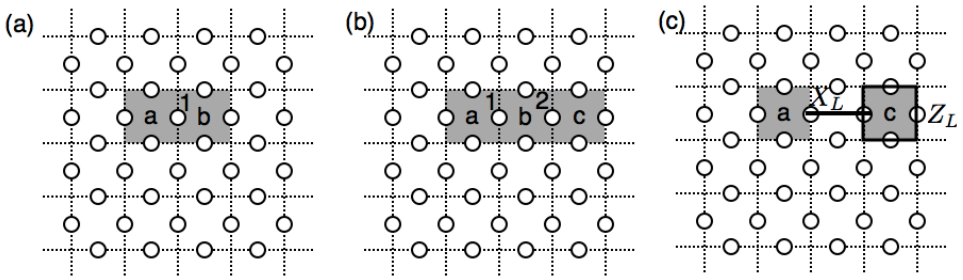


Figure 2.2: (a) A pair of primal defects a and b is introduced by measuring a qubit 1 in the X basis. (b) A neighboring defect c is generated by measuring a qubit 2. (c) The defects are separated by measuring the operator A_b. The logical Pauli operators X_L and Z_L are defined.

stabilizer state is a rank 1 state. In order to encode a logical qubit, we introduce a pair of primal defects a and b by measuring a qubit 1 in the X basis as shown in Fig. 2.2 (a). By this measurement the two face operators A_a and A_b, which are not commutable with the measurement, are removed from the stabilizers. However, the product A_aA_b is still in the stabilizer group. We can move the primal defect b as follows. A qubit 2 is measured in the X basis to generate a neighboring primal defect c as shown in Fig. 2.2 (b). Then, as shown in Fig. 2.2 (c), the operator A_b is measured to remove the defect b (A_b is revived as a stabilizer). As a result, the two primal defects are separated as a and c. We note that A_a and A_c do not belong to the stabilizer group, but A_aA_c is a stabilizer. Here we can define the logical Pauli operators X_L and Z_L for the pair of the separated primal defects as shown in Fig. 2.2 (c). These two logical operators, which are anti-commutable with each other, are commutable with all the stabilizers. Similarly to the pair of primal defects, we can create a pair of dual defects by removing the vertex operators from the stabilizer group (see Fig. 2.3).

Now we have two types of logical qubits, the primal and dual pairs of defects. We can perform the logical CNOT gate for these two logical qubits by braiding a defect around the other type of defect as shown in Fig. 2.4. Here we note that any trivial loop operators, which do not contain any defects, belong to the stabilizer group. Thus the multiplication of the trivial loop operator in Fig. 2.4 (b) does not change the logical states. As a result, the logical operator $X_L \otimes I_L$ before the braiding is equivalent to $X_L \otimes X_L$ after the braiding as shown in Fig. 2.4 (c). Similarly we can show that $I_L \otimes Z_L$ is transformed to $Z_L \otimes Z_L$ under the braiding. These commutation relations are the same as those between

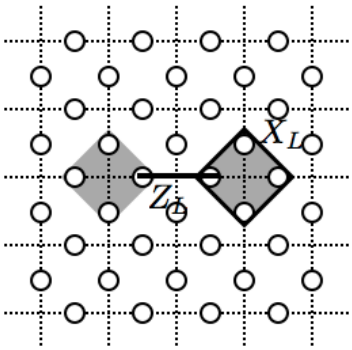


Figure 2.3: A pair of dual defects and the logical operators.

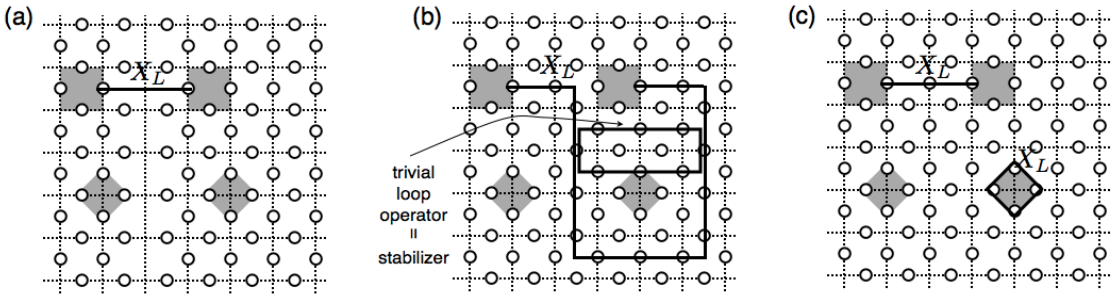


Figure 2.4: (a) Pairs of primal and dual defects. The logical Pauli operator X_L is defined as the chain which connects the two primal defects. (b) A primal defect (right) is braided around a dual defect (right). The trivial loop operator is a stabilizer operator, and acts trivially on the code state. (c) The logical Pauli operator $X_L \otimes I_L$ after the braiding is equivalent to the correlated Pauli operator $X_L \otimes X_L$.

the CNOT gate and Pauli operators. Accordingly, we can conclude that the braiding executes the logical CNOT gate operation. By combining the logical CNOT gates, state preparations and measurements, we can perform universal computation on the surface [92, 93, 94, 95].

Suppose that multiple errors occur simultaneously. Then, if the recovery operation forms a topologically non-trivial loop (i.e., logical Pauli operator), then the error correction is failed. Such a logical error probability can be decreased by enlarging the size of the defect. In other words, we can change the size of the code according to the size of the defect (surface). This is one of the most distinct points from the concatenated QEC codes.

The most striking property of the surface code is that all the stabilizer generators

are defined locally in Eq. (2.83). This property enables us to implement the syndrome measurements with only nearest-neighbor two-qubit gates. The fault-tolerant topological computation in two dimensions with nearest-neighbor two-qubit gates provides a high noise threshold $\sim 0.75\%$, in spite of its strong geometrical constraint [93, 94]. Furthermore, the syndrome measurements can be embedded into the two-dimensional cluster states [92, 96]. The logical operations such as the braiding can be implemented in one-way computation by adding an extra dimension for the time evolution. Thus fault-tolerant topological computation can also be executed by single-qubit measurements on a three-dimensional cluster states with a high noise threshold $\sim 0.67\%$ [92, 94]. Recently, the surface code and topological computation have been investigated against photon loss errors [97, 98, 99].

2.2.5 Postselected computation

We finally mention a different approach, namely *postselected computation* [20], which is closely related to the main theme of this thesis. In the standard fault-tolerant computation, as we have seen so far, errors detected in the QEC gadgets are corrected according to the syndrome. Instead, in the postselected computation, if any infections of errors are found in the syndrome, the gate operation is discarded. Then the computation is restarted from the beginning. For this purpose, the capability of correcting one error or more (i.e., distance three or further) is not necessarily required. One may use, for instance, the four-qubit error detection code with distance two, which encodes two logical qubits into four physical qubits. The stabilizer generators and logical Pauli operators are given as follows:

$$\begin{array}{rcccc} S_1 & = & X & X & X & X \\ S_2 & = & Z & Z & Z & Z \\ X_L^{(1)} & = & X & X & I & I \\ Z_L^{(1)} & = & Z & I & Z & I \\ X_L^{(2)} & = & X & I & X & I \\ Z_L^{(2)} & = & Z & Z & I & I \end{array} \tag{2.84}$$

where $X_L^{(i)}$ and $Z_L^{(i)}$ $(i = 1, 2)$ denotes the logical Pauli operators on the ith logical qubit. Since all single X, Y, and Z errors anti-commute with the stabilizers, we find that any single qubit error occurs on the code states. Accordingly, by postselecting the successful gate operations, one can realize a reliable logical gate operation on the four-qubit code. A serious drawback of postselection is that the logical operations become

nondeterministic (probabilistic). If we perform a whole computation with postselection, the success probability is diminished exponentially. Thus further ingredient is required for scalable computation.

Emanuel Knill settled this problem by switching to the standard computation at a sufficiently high concatenation level. That is, postselected computation is used to encode a QEC code which has a high capacity to correct errors, and subsequently the lower codes are decoded. Then, the standard fault-tolerant computation is executed by using the high-performance QEC code. The postselected computation costs huge resources, but it is a constant overhead. This idea is very promising to achieve a high noise threshold, although we have to improve the overhead for practical interest.

The main motivation of this thesis is to construct a scalable fault-tolerant scheme, which makes use of postselection for a high noise threshold, but restraints the resources usage to a reasonable level. As noted previously, if postselection is employed, the logical (two-qubit) gates become nondeterministic. This situation is somewhat similar to the linear optical quantum computer, where two-qubit gates are intrinsically nondeterministic. This problem can be settled by using a unique feature of one-way computation [41, 42, 49, 61, 62]. Motivated by these results on one-way computation, in the following Chapters, we present novel methods, which are beyond the naive postselected computation.

Chapter 3

Cluster-based architecture for fault-tolerant quantum computation

In this chapter, we present a detailed description of an architecture for fault-tolerant quantum computation, which is based on the cluster model of encoded qubits. In this cluster-based architecture, concatenated computation is implemented in a quite different way from the usual circuit-based architecture where physical gates are recursively replaced by logical gates with error-correction gadgets. Instead, some relevant cluster states, say fundamental clusters, are recursively constructed through verification and postselection in advance for the higher-level one-way computation, which namely provides error-precorrection of gate operations. A suitable code such as the Steane seven-qubit code is adopted for transversal operations. This concatenated construction of verified fundamental clusters has a simple transversal structure of logical errors, and achieves a high noise threshold $\sim 3\%$ for computation by using appropriate verification procedures. Since the postselection is localized within each fundamental cluster with the help of deterministic bare controlled-Z gates without verification, divergence of resources is restrained, which reconciles postselection with scalability.

3.1 Introduction

In order to implement reliable computation in physical systems, either classical or quantum, the problem of noise should be overcome. Particularly, fault-tolerant schemes have been developed based on error correction in quantum computation [10, 11, 12, 36, 79, 80, 83, 100]. In the usual quantum error correction (QEC), error syndromes are detected on encoded qubits, and the errors are corrected according to them. The noise thresholds for

fault-tolerant computation are calculated to be about $10^{-6} - 10^{-3}$ depending on the QEC protocols and noise models [13, 14, 15, 16, 17, 19, 36, 81, 83, 88, 100]. A main motivation for QEC comes from the fact that in the circuit model the original qubits should be used throughout computation even if errors occur on them.

On the other hand, more robust computation may be performed in measurement-based quantum computers [20, 38, 39, 41, 42, 101, 102, 103, 104]. Teleportation from old qubits to fresh ones is made by measurements to implement gate operations, and the original qubits are not retained. An interesting fault-tolerant scheme with error-correcting teleportation is proposed based on encoded Bell pair preparation and Bell measurement, which achieves high noise thresholds $\sim 3\%$ [20, 104]. The cluster model or one-way computer [41, 42] should also be considered for fault-tolerant computation. A highly entangled state, called a cluster state, is prepared, and gate operations are implemented by measuring the qubits in the cluster with feedforward for the postselection of measurement bases. This gate operation in the cluster model may be viewed as the one-bit teleportation [39]. A promising scheme for linear optical quantum computation is proposed, where deterministic gates are implemented by means of the cluster model [49]. Fault-tolerant computation is built up for this optical scheme by using a clusterized version of the syndrome extraction for QEC [83]. The noise thresholds are estimated to be about 10^{-3} for photon loss and 10^{-4} for depolarization [61, 62]. The threshold result is also argued by simulating the QEC circuits with clusters [58, 59, 60]. Furthermore, topological fault-tolerance in cluster-state computation is investigated in a two-dimensional nearest-neighbor architecture, where a high noise threshold $\sim 0.75\%$ is obtained in spite of its strong physical constraint [93, 94]. Some direct approaches are, on the other hand, considered for the fault-tolerant one-way computation [28, 105, 106], though there seems to be a problem for scalability.

In this chapter we present a systematic and comprehensive description of an architecture for fault-tolerant quantum computation, namely the cluster-based architecture, which has been proposed recently to reconcile postselection with scalability by virtue of one-way computation [29]. Specifically, the fault-tolerant computation is implemented by concatenated construction and verification of logical cluster states via one-way computation with postselection. A number of cluster states are constructed in parallel with error detection, and the unsuccessful ones are discarded, selecting the clean cluster states. The error-correcting teleportation (or its cluster version) [20, 104, 105, 106] requires a high-fidelity preparation of Bell state. It is also considered that improved ancilla preparation

increases the noise threshold [27, 107]. In the present cluster-based architecture [29], even gate operations as logical cluster states are prepared and verified by postselecting the lower-level computation to reduce the errors efficiently (see also Ref. [28] for an early idea). This is quite distinct from the usual circuit-based QEC architectures, including the error-correcting teleportation, where the errors are corrected after noisy gate operations.

While high-fidelity state preparation is achieved by postselection, huge resources are generally required due to the exponentially diminishing net success probability according to the computation size. This is a serious obstacle for scalability in the postselecting schemes [20, 28, 104]. Here, we succeed in overcoming this problem in postselection by presenting a systematic method of concatenation to construct logical cluster states through verification, where the unique feature of the cluster-model computation is fully utilized. As described in detail later, the necessary postselections are minimized and localized by dividing a whole cluster state into some fundamental clusters with the help of controlled-Z (CZ) gates without verification, say bare CZ gates. This enables the off-line gate operations prior to the computation as the verified logical cluster states, and provides a scalable concatenation with postselection in the cluster-model computation. The concatenated construction of verified clusters is implemented with transversal (bitwise) operations by adopting a suitable code such as the Steane seven-qubit code, which belongs to a class of stabilizer codes of Calderbank-Shor-Steane (CSS) [79, 80, 81]. The logical measurements of Pauli operators as well as the Clifford gates, H, S and CZ, are implemented transversally on such a quantum code. The non-Clifford $\pi/8$ gate is even operated for universal computation by preparing a specific qubit and making a transversal measurement [28, 105]. By exploiting this good transversal property, the cluster-based architecture has a simple structure of logical errors in concatenation to estimate readily the noise threshold. A high noise threshold $\sim 3\%$ can be achieved by using appropriate verification procedures with postselection. Furthermore, the resources usage is moderate, being comparable to or even less than those of the circuit-based QEC architectures.

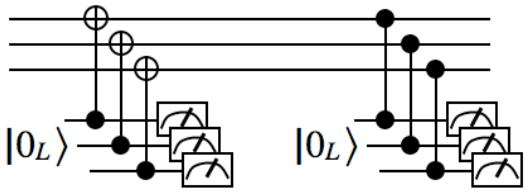
The rest of this chapter is organized as follows. In Sec. 3.2 we briefly review the usual fault-tolerant quantum computation with circuit-based QEC. In Sec. 3.3 we introduce the main concept of cluster-based architecture by considering a simple model preliminarily. In Sec. 3.4 we present a detailed description of an efficient architecture for the concatenated construction of verified logical clusters. The fundamental clusters and verification protocols are suitably adopted there, namely the hexacluster, code states, single and dou-

ble verifications. Then, performance of the architecture is analyzed in Secs. 3.5, 3.6 and 3.7, with respect to the noise threshold and resources usage. Section 3.8 is devoted to a summary and conclusion. In the Appendix A we explain how to produce the cluster diagrams to construct the fundamental clusters with single and double verifications.

3.2 Circuit-based fault-tolerant architecture

We first review the usual fault-tolerant architecture based on the circuit-model computation with QEC. In comparison, this will be helpful to understand the distinct feature of the cluster-based fault-tolerant architecture, which will be investigated in the succeeding sections.

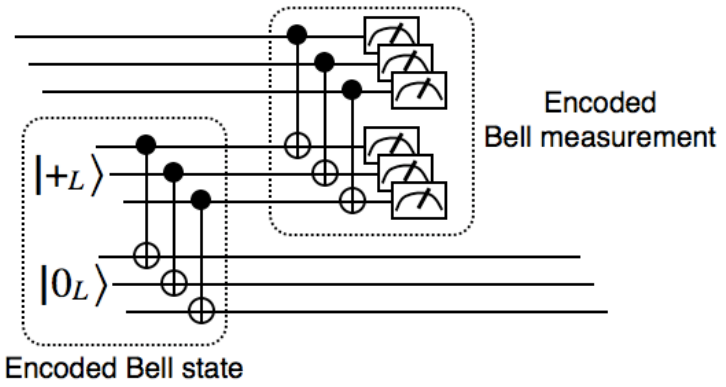
It is well known that by using QEC codes we can protect quantum information from errors which are caused by interaction with environment. Specifically, by adopting the stabilizer codes we can perform syndrome detection for recovery operation simply by measuring the stabilizer operators. Several QEC gadgets have been proposed to implement the stabilizer measurement in a fault-tolerant way [12, 20, 83]. A QEC gadget was first proposed by DiVincenzo and Shor, where cat states are used as ancillae for the syndrome measurement [12]. Subsequently, a relatively simple type of QEC gadget was proposed by Steane [83], where encoded ancilla states are used to extract the syndrome with transversal operations. Especially, in the case of CSS code the logical code states can be used as ancilla states. For example, the following circuit executes the Z and X error syndrome extractions by using the ancilla $|0_L\rangle$ states,



(3.1)

where the code blocks are illustrated as though for a three-qubit code for simplicity. In order to extract reliable error information, the syndrome extraction is repeated for some times. An optimized way to extract the syndrome information was also proposed in Ref. [85], where the subsequent syndrome extraction is conditionally performed according to the preceding syndrome information. Another interesting QEC gadget based on telepor-

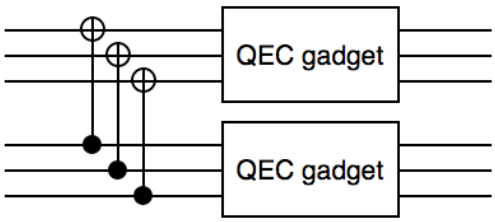
tation was proposed by Knill [20], which is illustrated as follows:



(3.2)

Here, the encoded data qubit is teleported to the fresh encoded qubit of the ancilla Bell state. The outcome of the encoded Bell measurement to complete the teleportation provides sufficiently the syndrome information, namely error-detecting or error-correcting teleportation. Thus, it is not necessary to repeat the syndrome extraction in this QEC gadget. The outcome of the Bell measurement is properly propagated to the subsequent computation as the Pauli frame [20, 61, 62].

Concatenated computation with QEC gadgets can be employed to achieve high accuracy for logical gate operations. In the usual fault-tolerant architectures based on the circuit-model computation [13, 15, 16, 17], the concatenation is implemented by replacing a physical (lower-level) gate operation recursively with a logical (upper-level) one followed by QEC gadgets such as the circuits (3.1) and (3.2). It is illustrated for a controlled-NOT (CNOT) gate as follows:



(3.3)

Here, we note that any logical gate operation should be followed by the QEC gadgets for fault-tolerant computation. We may call this type of concatenation in terms of logical circuits the circuit-based concatenation or circuit-based fault-tolerant architecture.

3.3 Cluster-based fault-tolerant architecture

3.3.1 Main concept

The cluster-based architecture pursues logical cluster states with high fidelity for reliable computation, whereas the circuit-based architecture concerns logical circuits with high accuracy as described in the preceding section. (Here, the terms "circuit-based" and "cluster-based" refer to the type of fault-tolerant concatenation. They do not specify the physical-level computation.) In the cluster model, quantum computation is implemented through measurements of the logical qubits in cluster states. Thus, high fidelity cluster states directly mean the ability to perform quantum computation with high accuracy. It is, however, not a trivial task to prepare such large entangled states with high fidelity as cluster states of logical qubits encoded in a concatenated QEC code. This may be done by adopting postselection (or multipartite entanglement purification). That is, logical cluster states are constructed through verification process; they are discarded if infection of errors is found. It is expected generally that as the size of an entangled state gets large, the probability to pass the postselection decreases substantially. Thus, we have to design suitably the cluster-based architecture so as to make it scalable, while the postselection is made successfully. This dilemma between postselection and scalability in concatenation can be overcome by utilizing the unique feature of the cluster-model computation [29]. The key elements are as follows:

• **Fundamental clusters** with certain topologies, which are used to compose a whole cluster state to implement a desired computation.

• **Verification protocols**, as parts of cluster states, to postselect the successful one-way computation for the construction of fundamental clusters.

• **Transversal bare CZ gates** without verification, which are used to connect the fundamental clusters deterministically to construct the whole cluster state scalably.

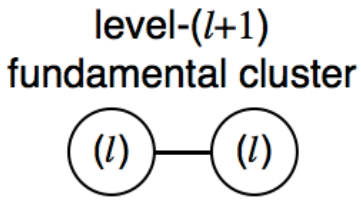
We need not verify the whole of a cluster state by postselection, which would have resulted in divergence of resources due to the diminishing success probability. Instead, at each concatenation level we divide the whole cluster state (one-way computation) into the fundamental clusters (gate operations and ancillae). The fundamental clusters are deterministically connected by the bare CZ gates which operate transversally on a suitable code such as the Steane seven-qubit code. As a result, the postselection is localized within each fundamental cluster, which reduces the resources usage dramatically, though

maintaining fault-tolerance of computation.

3.3.2 Preliminary model

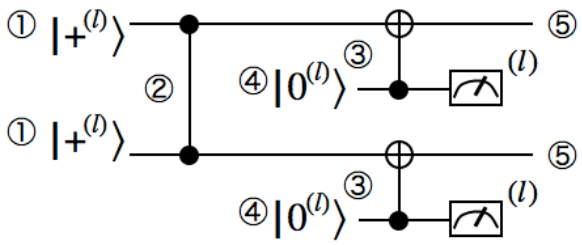
We consider preliminarily a simple model to illustrate the cluster-based architecture. At the same time, we introduce cluster diagrams, which are designed to describe properly the architecture.

We take one fundamental cluster as follows:



(3.4)

Henceforth we suitably define level-$(l+1)$ fundamental clusters as cluster states of level-l qubits in concatenation of a QEC code. (Level-0 qubits are physical ones.) In this model the level-$(l+1)$ fundamental cluster (3.4) consists of two level-l qubits connected with a CZ gate. We construct this level-$(l+1)$ fundamental cluster through a verification protocol as given in the following circuit:

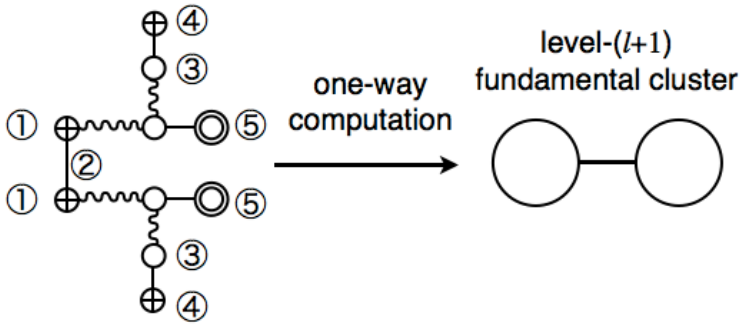


(3.5)

The two-qubit cluster is formed from the two level-l logical $|+^{(l)}\rangle$ qubits (①) through the CZ gate operation (②). The errors which are introduced to these two qubits before and during the CZ gate operation are detected by using a sort of the Steane's QEC gadget (③) with the ancilla $|0^{(l)}\rangle$ qubits (④). This verification protocol is implemented with postselection to obtain the level-$(l+1)$ fundamental cluster (3.4) with higher fidelity (⑤).

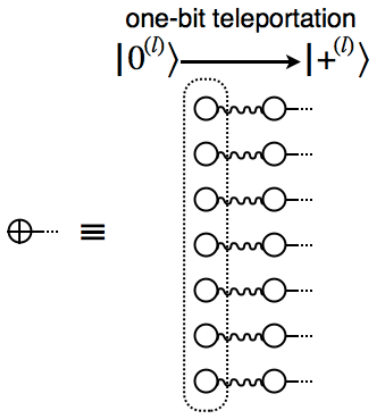
In the cluster-based architecture, the entanglement operation with verification to construct the level-$(l+1)$ fundamental cluster is implemented by one-way computation on a certain cluster state which is made by combining the level-l fundamental clusters with the transversal bare CZ gates. Specifically, the process (3.5) to obtain the fundamental

cluster (3.4) is described in terms of a cluster diagram as follows:



(3.6)

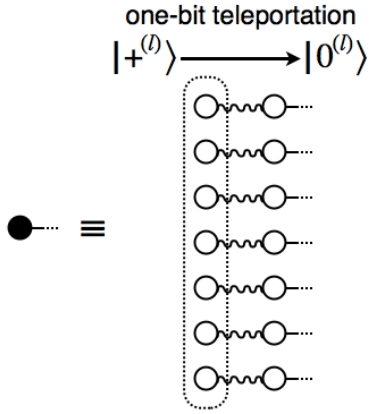
Here, the elements corresponding to those in the circuit (3.5) are labeled the same numbers ① – ⑤. We occasionally use the two-dimensional diagrams such as (3.6) to abbreviate the three-dimensional arrays to represent the whole cluster states by omitting the coordinate for the code blocks according to the encoding rules as explained below. [The whole three-dimensional array of (3.6) will be illustrated later.] The wavy lines in the diagram (3.6) indicate the bare CZ gates acting transversally on the level-$(l-1)$ qubits composing the level-l fundamental clusters. The output qubits (⑤) are denoted by ⊙ as the verified level-$(l+1)$ fundamental cluster. The operation for encoding and transferring the level-l code state $|+^{(l)}\rangle$ is described by $\oplus$ symbolically:



(3.7)

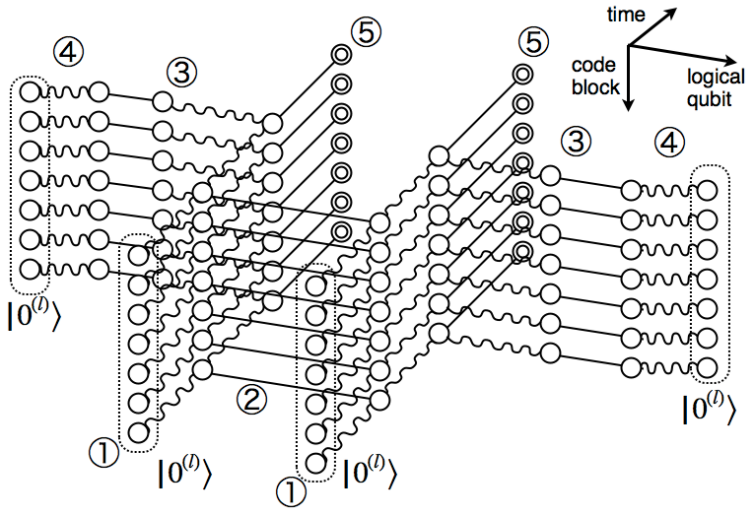
Here, the level-$(l-1)$ qubits surrounded by the dotted line form the level-l code state (cluster) $|0^{(l)}\rangle$. They are teleported upon measurements to another block of qubits as $|+^{(l)}\rangle$ by a Hadamard operation $|+^{(l)}\rangle = H|0^{(l)}\rangle$ with bare CZ gates (one-bit teleportation). The encoding operation of the level-l code state $|0^{(l)}\rangle$ is also described by ● symbolically for

the later use:



(3.8)

By applying the $\oplus$ encoding (3.7), the full three-dimensional array of the diagram (3.6) is obtained with the axes corresponding to the code blocks, logical qubits and time as follows:



(3.9)

Here, we observe that the level-$(l+1)$ fundamental cluster (3.4) is constructed through the verification by using 5×7 level-l fundamental clusters (3.4) and 4 level-l logical qubits $|0^{(l)}\rangle$ which are suitably connected with $(4+4) \times 7$ level-$(l-1)$ bare CZ gates.

As seen in the diagrams (3.7) and (3.8), the level-l code states $|0^{(l)}\rangle$ and $|+^{(l)}\rangle$ are used for the encoding operations. They are given as the cluster states of level-$(l-1)$ qubits, which are similar to the fundamental cluster (3.4). [See the diagrams (3.12) and (3.13) in the next section.] We can prepare these cluster states for $|0^{(l)}\rangle$ and $|+^{(l)}\rangle$ by combining some copies of the level-l fundamental cluster (3.4) with the level-$(l-1)$ bare CZ gates. (Here, we do not present their preparation explicitly for this preliminary model.) An alternative option is to include the level-l code states $|0^{(l)}\rangle$ and $|+^{(l)}\rangle$ in the set of level-l

fundamental clusters, as will be adopted in the next section for an efficient construction of fundamental clusters with high fidelity.

The circuit (3.5) is executed in the diagram (3.6) or (3.9) by measuring the level-$(l-1)$ qubits except for the output $\circledcirc$ qubits. Then, the syndrome information is extracted from the measurement outcomes (③ and ④). If this level-l syndrome is found to be correct, we keep the output $\circledcirc$ qubits (⑤) as the verified level-$(l+1)$ fundamental cluster. Otherwise, we discard the unsuccessful outputs. This one-way computation completes one concatenation; the level-$(l+1)$ fundamental cluster as the entangled set of output level-l qubits ($\circledcirc$'s) has been constructed and verified by using the level-l fundamental clusters with bare CZ gates.

We produce many copies of the fundamental cluster by performing the above procedure recursively up to a certain logical level high enough to achieve the expected accuracy. Then, we construct the whole cluster state to implement a desired computation by combining these copies of the fundamental cluster with the transversal bare CZ gates. The logical error of the transversal bare CZ gate on the concatenated code also becomes sufficiently small at the highest level. Thus, given the clean enough fundamental clusters at the highest level, the one-way computation is operated fault-tolerantly on the whole cluster state. In this preliminary model, however, the noise threshold will be rather low, since the verification protocol is not optimal, and some of the qubits are connected doubly to the bare CZ gates. A more efficient architecture will be described in the next section, which achieves a high noise threshold $\sim 3\%$.

3.3.3 Unique features

We should mention that the role of bare CZ gates in the cluster-based architecture provides the essential distinction from the circuit-based architecture. The postselection with QEC gadgets can really achieve high accuracy for computation. However, in the circuit-based concatenation the postselection of gate operations should be performed in the ongoing computation (even if the error-detecting teleportation is utilized with off-line preparation of ancilla states [20]). Thus, if errors are detected, the computation should be restarted from the beginning, which results in divergence of resources usage. This is because in the circuit-based architecture any logical gate operation is necessarily followed by QEC gadgets at each concatenation level, as seen in Sec. 3.2.

Instead, in the cluster-based architecture bare CZ gates, which are not accompanied by

QEC gadgets, are partially used for the one-way computation to implement the construction process, while fault-tolerance can be ensured by the verification and postselection of fundamental clusters. The logical cluster states are really postselected *off-line and locally* since the whole cluster is divided into the fundamental clusters with the help of bare CZ gates. When clean enough fundamental clusters are just constructed, we connect them with bare CZ gates deterministically, and then start the computation. The fundamental clusters, which represent the gate operations, have been constructed successfully in advance by removing sufficiently the errors via the postselection in the lower-level one-way computation, before starting the computation at the higher level. Thus, we may call this verification process as *preselection* or *error-precorrection* of gate operations. Here, it should be noted that the postselection for the whole cluster state or computation, without the use of bare CZ gates, increases exponentially the resources according to the computation size. In the present architecture postselection and scalability are reconciled quite naturally by using the cluster-model computation.

The cluster-based architecture also exploits a good transversal property by adopting a suitable code such as the Steane seven-qubit code. That is, the operations on the physical qubits are all transversal, and really limited after the verification process at the lowest (physical) level. In fact, as seen in the diagram (3.6), any direct operation is not implemented on the output qubits (◎'s) through the verified construction of fundamental cluster. The desired entanglement among them to form the fundamental cluster at the next level is rather generated via one-bit teleportation in the one-way computation. Thus, they inherit transversally the errors on the constituent physical-level qubits, up to the Pauli frame information from the one-way computation for cluster construction. Then, these output qubits composing the fundamental clusters undergo the transversal bare CZ gates and measurements at the next level for the first time. This transversal property provides a simple structure of logical errors in concatenation to estimate readily the noise threshold. In this respect, the cluster-based architecture presents a practical way to construct large entangled states, including the concatenated code states and fundamental clusters, the errors of which are described in a good approximation by the homogeneous errors on the constituent physical-level qubits [27]. The details will be demonstrated in the following sections.

3.4 Concatenated construction of verified cluster states

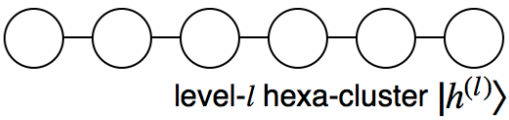
We now introduce an efficient architecture for fault-tolerant concatenation by adopting a set of suitable fundamental clusters and elaborate verification protocols. It is really designed to achieve high noise threshold by taking full advantage of the present cluster-based scheme. As seen in the diagram (3.6), some of the qubits are connected doubly to the bare CZ gates for the cluster construction in the preliminary model. This lowers the noise threshold substantially. Thus, the topologies of the fundamental clusters should be chosen so as to limit suitably the use of bare CZ connections (at most one bare CZ gate to each qubit) and redundant qubits for the cluster construction. It should also be noted that the errors on the resultant fundamental clusters are not detected after the construction is completed. This requires that the verification protocols should detect fully the first-order errors except for some of the errors introduced by the final few operations, which are inevitably left on the output states.

3.4.1 Fundamental clusters

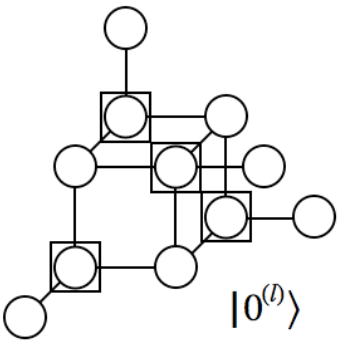
We adopt the following states as the level-l fundamental clusters:

$$|h^{(l)}\rangle, |0^{(l)}\rangle, |+^{(l)}\rangle. \tag{3.10}$$

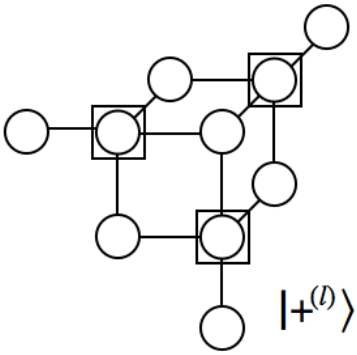
They are depicted in terms of the cluster diagrams as



(3.11)



(3.12)



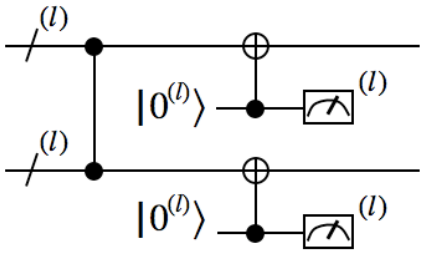
(3.13)

where the circles denote the level-$(l-1)$ qubits, and the boxed qubits are measured for Hadamard operations to obtain $|0^{(l)}\rangle$ and $|+^{(l)}\rangle$. The hexacluster $|h^{(l)}\rangle$ is a cluster state of six level-$(l-1)$ qubits which are connected linearly with CZ gates. This hexacluster represents an elementary unit of gate operations as seen later. The level-l concatenated code states $|0^{(l)}\rangle$ and $|+^{(l)}\rangle$ are also taken as the fundamental clusters in this architecture. They are used as ancillae for encoding and syndrome detection.

3.4.2 Single and double verifications

The level-$(l+1)$ fundamental clusters are constructed by operating the CZ gates on the level-l qubits. These gate operations inevitably introduce errors on the output states. Thus, as seen in Sec. 3.3, we verify and postselect the output states for the high fidelity construction. Specifically, we detect the errors efficiently by combining two verification gadgets, namely single and double verifications.

The CZ gate operation with single verification is given in terms of a circuit as

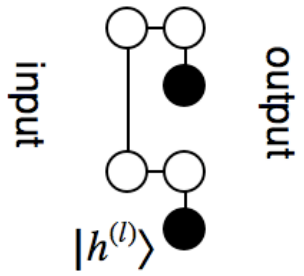


(3.14)

where each dashed line with index (l) indicates that seven level-$(l-1)$ wires are contained there. The single verification is the same as the protocol (3.5) for the model in Sec. 3.3. The Z error on the level-l qubit is detected by the Z syndrome extraction after the CZ gate operation. Furthermore, the preceding X error on the level-l qubit is detected by

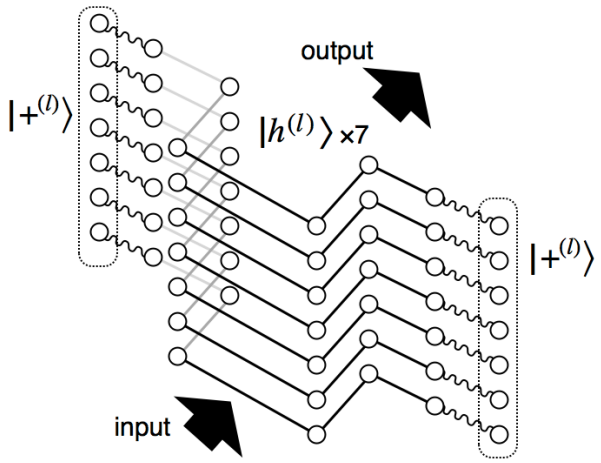
the Z syndrome extraction for the other level-l qubit since it is propagated through the CZ gate as a Z error.

The cluster diagram for the single verification (3.14) is given with the fundamental clusters as



(3.15)

where the ●'s denote the encoding of $|0^{(l)}\rangle$ for the syndrome extraction in the circuit (3.14). By considering the ● encoding (3.8), the single-verification diagram (3.15) is fully illustrated in terms of a cluster state of level-$(l-1)$ qubits as

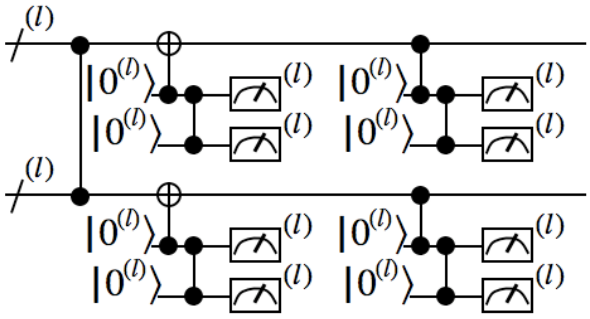


(3.16)

which may be compared with the diagram (3.9) in the preliminary model. Here, we observe that the level-l CZ gate operation with single verification, as given in the circuit (3.14) and diagram (3.15), is implemented by using $7|h^{(l)}\rangle$'s, $2|+^{(l)}\rangle$'s and 2×7 level-$(l-1)$ bare CZ gates.

In order to remove sufficiently the errors in the final stage of construction, we implement the double verification, which may be viewed as a sophistication of the Steane's QEC gadget in the circuit (3.1). The CZ gate operation with double verification is described

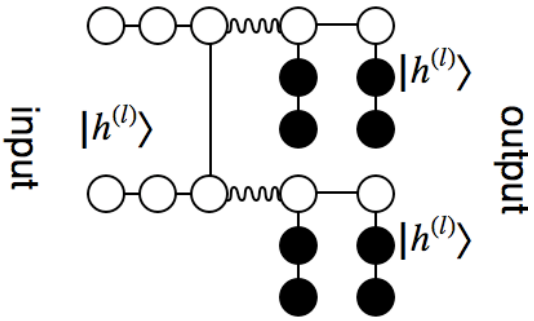
as follows:



(3.17)

Here, the Z error verification through a CNOT gate is followed by the X error verification through a CZ gate for high fidelity. Furthermore, the error propagation from the primary ancilla qubit $|0^{(l)}\rangle$ to the data qubit through the two-qubit gate (CNOT or CZ) is prohibited in the leading order by inspecting the primary $|0^{(l)}\rangle$ with the secondary $|0^{(l)}\rangle$. In fact, this double verification with the primary and secondary ancilla states has been applied recently to implement a high-performance recurrence protocol for entanglement purification [30], where its optimality for detecting the first-order errors is discussed. We also note that the single and double verifications in (3.14) and (3.17) both remove the preceding errors through the CZ gate by the syndrome extractions for the two level-l qubits.

Similar to the single-verification diagram (3.15), the circuit (3.17) for the double verification is implemented by a cluster diagram as follows:

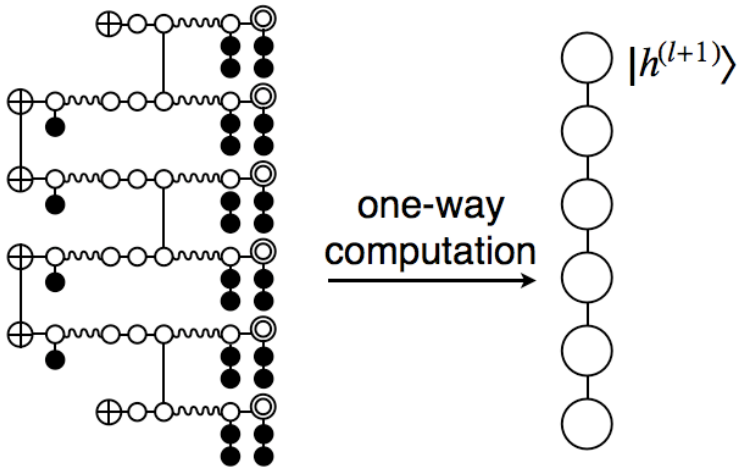


(3.18)

The full diagram for (3.18) is generated by considering the ● encoding of $|0^{(l)}\rangle$ in (3.8), similarly to the single-verification diagram (3.16). We realize in the diagram (3.18) that the level-l CZ gate operation with double verification is implemented by combining 3×7 $|h^{(l)}\rangle$'s and $8|+^{(l)}\rangle$'s with $(8+2) \times 7$ level-$(l-1)$ bare CZ gates.

3.4.3 Concatenated cluster construction

The level-$(l+1)$ fundamental clusters are constructed from the level-l ones via one-way computation. In order to achieve high fidelity, the CZ gate operations with single and double verifications are combined by using the bare CZ gates in a suitable way; (i) each qubit has at most one bare CZ connection (wavy line), and (ii) the output ◎ qubits to form the level-$(l+1)$ fundamental clusters have no bare CZ connection, and they are doubly verified in the final stage of construction. Specifically, the level-$(l+1)$ hexacluster $|h^{(l+1)}\rangle$ is constructed as follows:

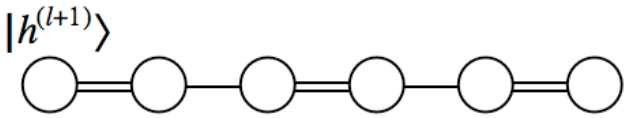


(3.19)

The 6 $|+^{(l)}\rangle$'s are transferred by the $\oplus$ encoding (3.7), and they are entangled through 2 CZ gates with single verification (3.15) and 3 CZ gates with double verification (3.18) to form the $|h^{(l+1)}\rangle$ (the output 6 ◎ qubits at the level l). This one-way computation to construct the $|h^{(l+1)}\rangle$ is implemented by measuring the level-$(l-1)$ qubits, except those for the output ◎'s, in the three-dimensional diagram for (3.19). [The full diagram is generated with the code-block axis supplemented according to the encodings (3.7) and (3.8), as the diagrams (3.9) and (3.16).] The level-l syndromes are extracted through the measurements of the ancilla encoded ● qubits. If all the level-l syndromes are correct, the entangled set of six level-l ◎ qubits survive as a verified $|h^{(l+1)}\rangle$.

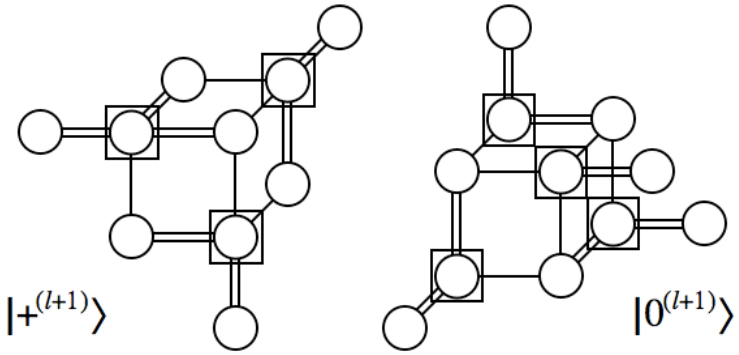
Since the cluster diagrams such as (3.19) look somewhat complicated, we introduce suitably the reduced diagrams by omitting the time axis and qubits measured in the

one-way computation. The hexacluster construction (3.19) is described as follows:



(3.20)

Here, the single and double lines indicate the single and double verifications, respectively, and it is understood that the single verifications are always done before the double verifications. We construct similarly the fundamental clusters $|0^{(l+1)}\rangle$ and $|+^{(l+1)}\rangle$ as

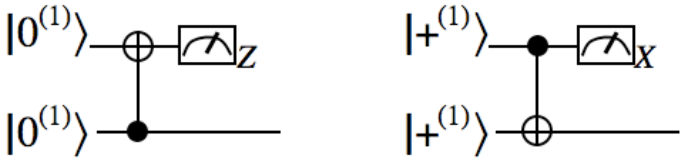


(3.21)

where the boxed level-l qubits are measured transversally in the X basis for Hadamard operations. We see that in these reduced diagrams all the qubits have at least one double-line connection, that is they are doubly verified in the final stage of construction. We can produce systematically the construction processes such as (3.19) from the reduced diagrams. The details are described in the Appendix A.

At the beginning of concatenation, the construction of the level-2 fundamental clusters by the physical-level computation is somewhat different from the constructions at the higher levels. This is because the verified level-1 fundamental clusters are not available by definition from the lower-level construction. It may be suitable to adopt the circuit-model computation at the physical level since both CNOT and CZ gates are deterministically available. The level-1 $|0^{(1)}\rangle$ and $|+^{(1)}\rangle$ are first encoded and verified against the Z and X errors by measuring the X and Z stabilizers, respectively. They are, however, not clean enough for the present purpose. We secondly verify the X and Z errors on the $|0^{(1)}\rangle$ and

$|+^{(1)}\rangle$, respectively, as follows:



(3.22)

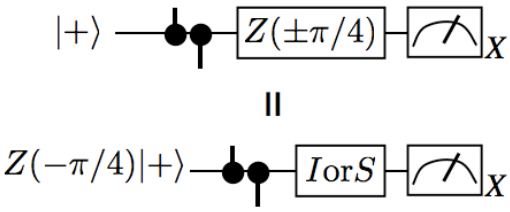
This operation is the same as the multipartite entanglement purification [86, 87]. Then, we construct the level-2 fundamental clusters $|h^{(2)}\rangle$, $|0^{(2)}\rangle$ and $|+^{(2)}\rangle$ from these verified level-1 qubits $|0^{(1)}\rangle$ and $|+^{(1)}\rangle$ by implementing the circuits (3.14) and (3.17) with the bare CZ gates ($l = 1$) according to the reduced diagrams (3.20) and (3.21). It is also possible to perform the physical-level one-way computation by means of the cluster diagrams to implement the relevant circuits for the level-2 construction. Additional errors are, however, introduced lowering slightly the noise threshold since the extra operations are required for the CNOT gate operations in the one-way computation. This will be considered explicitly in Sec. 3.7.

3.4.4 Universal computation

The fundamental clusters are constructed through verification up to the highest logical level $\bar{l}$ to achieve the fidelity required for a given computation size. Then, we can perform accurately the computation with Clifford gates by combining the highest-level hexaclusters $|h^{(\bar{l}+1)}\rangle$ with the transversal bare CZ gates and performing the Pauli basis measurements of the level-$\bar{l}$ qubits in the cluster states. Furthermore, we can implement even non-Clifford gates for universal computation as explained below.

In the cluster model the operation $HZ(\theta) = He^{-i\theta Z/2}$ is implemented by the measurement in the basis $Z(\pm\theta)\{|+\rangle, |-\rangle\}$ with $\pm\theta$ to be selected according to the outcome of preceding measurements [41, 42]. The non-Clifford gates, e.g., the $\pi/8$ gate $= Z(\pi/4)$, however, do not operate transversally even on the Steane seven-qubit code. Then, in order to implement the $\pi/8$ gate with a transversal measurement, we make use of the

equivalence as follows:



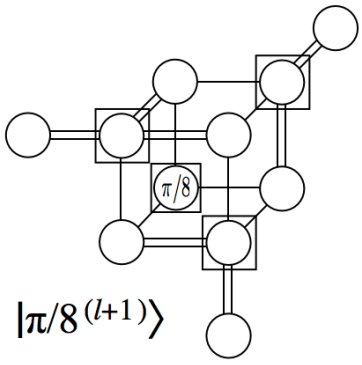
(3.23)

As a result, the operation $HZ(\pi/4)$ can be implemented by the preparation of the state $Z(-\pi/4)|+\rangle$ and the measurement with the I or $S = Z(\pi/2)$ operation (the selection of measurement basis X or $-Y = SXS^\dagger$). The preparation of $Z(-\pi/4)|+\rangle$ is reduced to that of $|\pi/8\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ based on the relation

$$Z(-\pi/4)|+\rangle = e^{i\phi}HS|\pi/8\rangle, \tag{3.24}$$

where ϕ is a certain phase. In this way we can implement the H, S, $\pi/8$ and CZ gates as a universal set by the transversal Pauli basis measurements of the level-$\bar{l}$ qubits, including $|\pi/8^{(\bar{l})}\rangle$, in the level-$(\bar{l}+1)$ cluster states [28, 105].

The level-1 $|\pi/8^{(1)}\rangle$ is encoded by the usual method [15, 16, 20]. Then, similarly to the other fundamental clusters the upper-level $|\pi/8^{(l+1)}\rangle$ $(l \geq 1)$ is encoded with the lower-level $|\pi/8^{(l)}\rangle$, as shown in the following reduced diagram:



(3.25)

where the $\pi/8$ circle indicates the transfer of $|\pi/8^{(l)}\rangle$ through a H rotation, similarly to the $\bullet$ and $\oplus$ encoding operations. The logical failure of $|5\pi/8^{(l+1)}\rangle$, however, cannot be detected in the construction of $|\pi/8^{(l+1)}\rangle$ because it has also the correct syndrome. Thus, this small mixture of $|5\pi/8^{(l+1)}\rangle$ is not reduced by the concatenation, though the constructed $|\pi/8^{(l+1)}\rangle$ is kept on the code space by verification, retaining the logical fidelity as the $|\pi/8^{(1)}\rangle$. This slightly noisy $|\pi/8^{(\bar{l})}\rangle$ $(l+1=\bar{l})$ is even useful to obtain the desired high fidelity $|\pi/8^{(\bar{l})}\rangle$ at the highest level by using the magic state distillation with Clifford operations [82, 108].

3.5 Noise threshold

We have described in the previous section how to construct the verified fundamental clusters in concatenation, which enables us to implement universal computation fault-tolerantly. In the following sections we investigate the performance of this cluster-based architecture, including a high noise threshold by postselection and reasonable resources usage for scalability.

The construction of fundamental clusters is performed via the one-way computation at the lower level. This provides readily the threshold condition for the cluster-based architecture: *The error probability for the measurement of each logical qubit, which composes the verified fundamental clusters, should be reduced arbitrarily by raising the concatenation level.* The errors in measuring the logical qubits are twofold: (i) the errors on the logical qubits themselves, and (ii) the errors on the Pauli frames, which are propagated as byproducts of one-way computation [41, 42]. The errors of (ii) are thus given by induction as some multiple of those of (i) in the leading order. We also note, as discussed in Sec. 3.3, that the cluster-based architecture exploits a good transversal property on a suitable code, which provides, in collaboration with the postselection, a simple concatenation structure of the logical errors in the verified fundamental clusters. Here, we estimate the noise threshold by considering these features of the cluster-based architecture. In this calculation we adopt the noise model as follows:

• A two-qubit gate is followed by $A \otimes B$ errors with probabilities p_{AB} ($A, B = I, X, Y, Z$, and $AB \neq II$).

• The physical qubits $|0\rangle$ and $|+\rangle$ are prepared as mixed states with an error probability p_p:

$$|0\rangle \rightarrow (1-p_p)|0\rangle\langle 0| + p_p|1\rangle\langle 1|, \tag{3.26}$$

$$|+\rangle \rightarrow (1-p_p)|+\rangle\langle +| + p_p|-\rangle\langle -|. \tag{3.27}$$

• The measurement of a physical qubit in the A (X, Y, Z) basis is described by positive-operator-valued measure (POVM) elements $\{M_A^+, M_A^-\}$ with an error probability p_M:

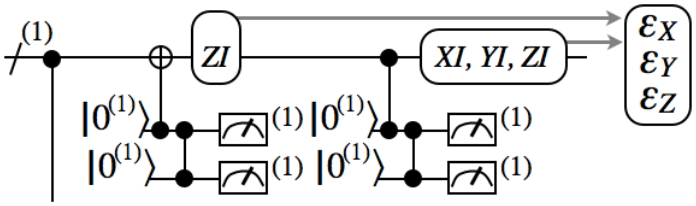
$$M_A^+ = (1-p_M)E_A^+ + p_M E_A^-, \tag{3.28}$$

$$M_A^- = (1-p_M)E_A^- + p_M E_A^+, \tag{3.29}$$

where $E_A^\pm = (I \pm A)/2$ are the projectors to the ± 1 eigenstates of the Pauli operator A, respectively.

3.5.1 Homogeneous errors in verified clusters

We first consider the errors on the level-0 (physical-level) qubits encoded in the level-2 fundamental clusters. Although the correlated errors are introduced in the encoding process of the level-1 qubits, they are detected and discarded by postselection sufficiently through the single and double verifications in the circuits (3.14) and (3.17) for the level-2 cluster construction. These verification protocols are implemented by the transversal operations. Thus, it is reasonably expected that the level-0 qubits encoded in these verified level-1 qubits, which compose the level-2 fundamental clusters, have independently and identically distributed (homogeneous) depolarization errors in the leading order [27]. Specifically, the homogeneous error probabilities ϵ_A $(A = X, Y, Z)$ for the level-0 qubits are determined by those p_{AB} for the physical two-qubit gates which are used transversally for the double verification in the final stage of construction. This is illustrated in the circuit (3.17) as



(3.30)

providing the homogeneous errors,

$$\epsilon_X = p_{XI}, \epsilon_Y = p_{YI}, \epsilon_Z \quad = \quad 2p_{ZI}, \tag{3.31}$$

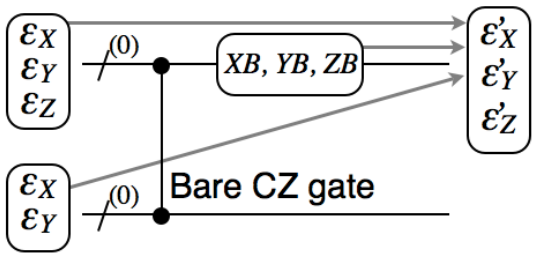
up to the higher-order contributions. The errors preceding the double verification, including the preparation error with p_p, are fully detected and discarded by postselection in the leading order, as discussed below the circuit (3.17).

The verified level-2 fundamental clusters are connected with the transversal bare CZ gates to construct the level-3 fundamental clusters as shown in the diagram (3.19). After the one-way computation with postselection, the output level-2 qubits are left successfully, composing the level-3 fundamental clusters. Here, it should be noted that the output level-2 qubits, ⊙'s in the diagram (3.19), are never touched directly in the level-3 cluster construction. Instead, the entanglement by the verified CZ gates is transferred via teleportation (one-way computation) transversally to the output level-2 qubits to form the verified level-3 fundamental clusters. Thus, each constituent level-0 qubit in these

entangled level-2 qubits inherits transversally the homogeneous errors ϵ_A in Eq. (3.31) after the double verification in the level-2 cluster construction. The above argument is extended recursively to the verified level-l fundamental clusters ($l \geq 2$). As a result, the errors in the verified fundamental clusters (before the bare CZ connections in the next-level construction) are reasonably described in terms of the homogeneous errors ϵ_A on the level-0 qubits. This fact really simplifies the error structure in the cluster-based architecture. Furthermore, the Pauli frame errors are removed in the leading order for the output qubits through the double verification. Thus, the cluster-based architecture provides a scalable way to construct a concatenated code state whose errors are well approximated by the homogeneous errors, which was assumed in Ref. [27].

3.5.2 Noise threshold calculation

We next consider the errors for the measurement of the logical qubits in the one-way computation to construct the verified fundamental clusters. The level-l clusters with the homogeneous errors ϵ_A on their constituent level-0 qubits are used for the level-$(l+1)$ cluster construction. As seen in the previous section, e.g., the diagram (3.16), some pairs of level-$(l-1)$ qubits in these level-l clusters are connected by the bare CZ gates. As a result, extra errors are added transversally to the constituent level-0 qubits through the bare CZ connection, as shown in the following diagram:



(3.32)

Then, the homogeneous errors after the bare CZ connection are given in the leading order as

$$\epsilon'_X = \epsilon_X + \sum_{B=I,X,Y,Z} p_{XB}, \tag{3.33}$$

$$\epsilon'_Y = \epsilon_Y + \sum_{B=I,X,Y,Z} p_{YB}, \tag{3.34}$$

$$\epsilon'_Z = \epsilon_Z + \epsilon_X + \epsilon_Y + \sum_{B=I,X,Y,Z} p_{ZB}. \tag{3.35}$$

Now we are ready to calculate the error probability for the measurement of the bare-connected level-l qubit which is implemented in concatenation by the transversal measurements of the constituent lower-level qubits. Consider first the level-1 qubits composing the level-2 fundamental clusters, which are measured in the level-1 one-way computation for the level-3 cluster construction. Note here that the level-0 qubits (constituents of the level-1 qubits) are not assigned the Pauli frames in the circuit-model computation at the physical level to construct the level-2 fundamental clusters. (Even if the cluster-model computation is adopted at the physical level, the Pauli frame error can be neglected in a good approximation, which is left only as the second-order error contribution after the double verification.) Thus, the measurement of the level-1 qubit is affected by the errors ϵ'_A on the level-0 qubits and the physical measurement error p_M. The logical error probability for the X measurement of the bare-connected level-1 qubit is then calculated in the leading order on the Steane seven-qubit code with distance 3 as

$$p_q^{(1)} \simeq {}_7\mathrm{C}_2(\epsilon'_Z + \epsilon'_Y + p_M)^2 \equiv {}_7\mathrm{C}_2(p_q^{(0)})^2, \tag{3.36}$$

where $p_q^{(0)}$ is defined as the error probability for the X measurement of the bare-connected level-0 qubit. It is apparent here that by choosing properly the physical basis the errors for the Z and Y measurements are arranged to be smaller than $p_q^{(0)}$ for the X measurement, i.e., $\epsilon'_Z \geq \epsilon'_Y \geq \epsilon'_X$.

The outcomes of the measurements of the level-1 qubits are propagated to the neighboring qubits by updating the Pauli frames according to the rule of one-way computation [41, 42]. Then, the errors on the measurement outcomes with the probability $p_q^{(1)}$ are accumulated during the computation. The blocks of seven output level-1 qubits (level-2 qubits) to form the level-3 fundamental clusters are, however, doubly verified in the final stage of one-way computation. Thus, the propagation of the preceding measurement errors as the Pauli frame error is prohibited by postselection in the leading order for these output level-1 qubits, as discussed in the circuit (3.17):

$$p_{\mathrm{Pauli}}^{(1)} \sim (p_q^{(1)})^2. \tag{3.37}$$

Subsequently, the level-2 one-way computation is performed by using the level-3 fundamental clusters to construct the level-4 fundamental clusters, where the constituent level-2 qubits are measured. Some of the level-2 qubits are connected with the transversal bare CZ gates for the first time in this computation. The measurement of the (bare-connected)

level-2 qubit is executed by measuring the (bare-connected) level-1 qubits transversally. The seven level-1 measurement outcomes together with the seven level-1 Pauli frames determine the level-2 measurement outcome. Then, by considering Eq. (3.37) the error probability for measuring the level-2 qubit after the bare CZ connection is given in the leading order as

$$p_q^{(2)} \simeq {}_7\mathrm{C}_2(p_q^{(1)} + p_{\mathrm{Pauli}}^{(1)})^2 \simeq {}_7\mathrm{C}_2(p_q^{(1)})^2. \tag{3.38}$$

As for the logical error left on the Pauli frame of each output qubit after the cluster construction, similarly to Eq. (3.37), it is reduced by the double verification as

$$p_{\mathrm{Pauli}}^{(l-1)} \sim (p_q^{(l-1)})^2 (l \geq 2). \tag{3.39}$$

Thus, the error probability $p_q^{(l)}$ for measuring the level-l qubit is calculated in concatenation as

$$p_q^{(l)} \simeq {}_7\mathrm{C}_2(p_q^{(l-1)})^2 \simeq ({}_7\mathrm{C}_2 p_q^{(0)})^{2^l}/{}_7\mathrm{C}_2. \tag{3.40}$$

The threshold condition is then given from Eq. (3.40) as

$$p_q^{(0)} = Dp_g < 1/{}_7\mathrm{C}_2, \tag{3.41}$$

and the noise threshold is estimated as

$$p_{\mathrm{th}} \simeq ({}_7\mathrm{C}_2 D)^{-1}, \tag{3.42}$$

where p_g represents the mean error probability for physical operations ($D \sim 1$). Typically with $p_{AB} = (1/15)p_g$ for ϵ'_A and $p_M = (4/15)p_g$ [104], where $D = 17/15$, the noise threshold is estimated approximately as $p_{\mathrm{th}} \simeq 0.04$.

3.5.3 Numerical simulation

We have made numerical calculations to confirm the above estimation of the error probability $p_q^{(l)}$ for measuring the logical qubit and the noise threshold p_{th} for computation by simulating the construction of fundamental clusters.

First, we have constructed the level-2 fundamental clusters according to the diagrams (3.20) and (3.21) by implementing the CZ operations with single and double verifications for the level-1 encoded qubits in the circuits (3.14) and (3.17) with bare CZ gates

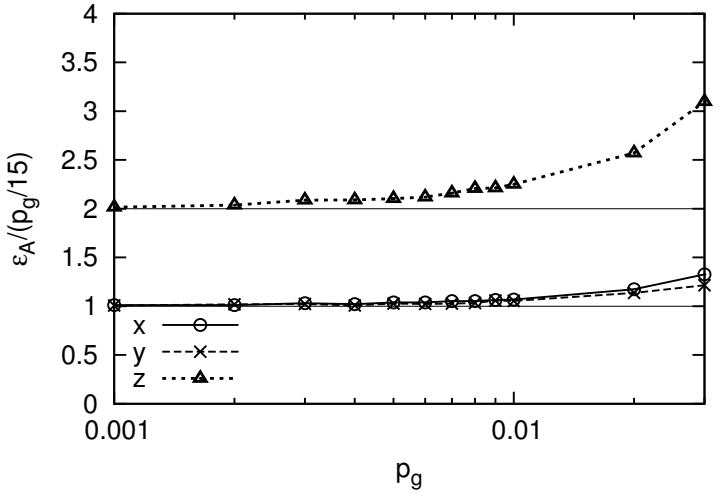


Figure 3.1: The error probabilities $\epsilon_A/(p_g/15)$ $(A = X, Y, Z)$ for each level-0 qubit are plotted as functions of the physical error probability p_g together with their leading values $\epsilon_X/(p_g/15) = \epsilon_Y/(p_g/15) = 1$ and $\epsilon_Z/(p_g/15) = 2$.

(transversal operation of physical CZ gates). Then, we have checked the error probabilities ϵ_A $(A = X, Y, Z)$ for each level-0 qubit which is contained in the output level-1 qubits as the verified level-2 fundamental clusters. In Fig. 3.1 $\epsilon_A/(p_g/15)$ are plotted as functions of the physical error probability p_g, where $p_{AB} = p_g/15$, $p_M = (4/15)p_g$ and $p_p = (4/15)p_g$ [104] are specifically adopted. In the case of $p_g < 1\%$ they are in good agreement with the leading values $\epsilon_X/(p_g/15) = \epsilon_Y/(p_g/15) = 1$ and $\epsilon_Z/(p_g/15) = 2$ in Eq. (3.31). On the other hand, in the case of $p_g > 1\%$ $\epsilon_A/(p_g/15)$ become larger due to the higher-order contributions, which are thus significant for $p_q^{(1)}$. It has been also checked for $p_g \leq 3\%$ that these errors are almost independent among the level-0 qubits; the correlated errors are one order of magnitude smaller than the independent ones even when the higher-order contributions are significant for ϵ_A. We have then evaluated the error probability $p_q^{(1)}$ for measuring the output level-1 qubit (component of the level-2 fundamental cluster) after operating the bare CZ gate on it. It is plotted in Fig. 3.2 as a function of p_g.

Next, we have constructed the level-3 fundamental clusters by simulating the one-way computation for the level-1 qubits (level-2 cluster states) in the diagrams such as (3.19) or their full three-dimensional versions. Then, we have calculated the error probabilities $p_{\rm Pauli}^{(1)}$ for the Pauli frames (X, Y, Z) of the level-1 qubit which is contained in the output level-2 qubit (component of the level-3 fundamental cluster). They are plotted in Fig. 3.2 as functions of p_g in comparison with the error probability $p_q^{(1)}$ for measuring the level-1

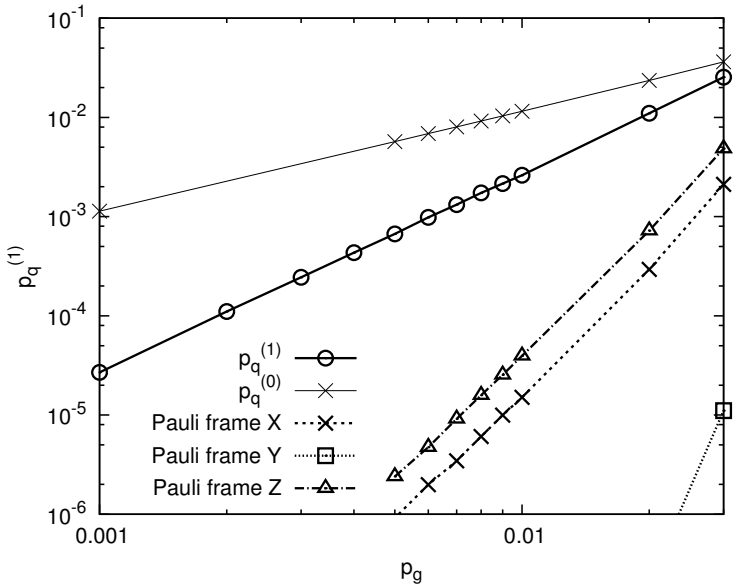


Figure 3.2: The error probability $p_q^{(1)}$ for measuring the level-1 qubit after the bare CZ connection is plotted as a function of the physical error probability p_g. The error probabilities $p_{\rm Pauli}^{(1)}$ for the Pauli frames (X, Y, Z) of the level-1 qubit are also plotted as functions of p_g in comparison with $p_q^{(1)}$. The upper-most line indicates $p_q^{(0)}$ in comparison to infer the threshold.

qubit. This result really confirms that $p_{\rm Pauli}^{(1)}$ is suppressed substantially by the double verification, to be of the second order of $p_q^{(1)}$, as shown in Eq. (3.37).

By using these values of $p_q^{(1)}$ and $p_{\rm Pauli}^{(1)}$ for the level-1 qubit, we have calculated the error probability $p_q^{(2)}$ for measuring the output level-2 qubit (component of the level-3 fundamental cluster) after the bare CZ connection. It is plotted as a function of p_g in Fig. 3.3 together with the leading term ${}_7{\rm C}_2(p_q^{(1)})^2$ (dotted line) as given in Eq. (3.38). (The error effect for $p_q^{(2)}$ due to the bare CZ connection is already taken into account transversally as a contribution in $p_q^{(1)}$.) Here, it is found that for $p_g > 1\%$ near the threshold the level-2 qubit error $p_q^{(2)}$ becomes significantly higher than its leading value (dotted line) due to the higher-order contributions including the Pauli frame error. The logical error probability, however, decreases through concatenation as $p_q^{(2)} < p_q^{(1)} < p_q^{(0)}$ for $p_g \leq 3\%$. This certainly indicates that the noise threshold $p_{\rm th}$ is about 3%, which is in reasonable agreement with the leading-order estimate in Eq. (3.42). The noise threshold $p_{\rm th} \sim 3\%$ of the present architecture is considerably higher than those of the usual circuit-based architectures with the Steane seven-qubit code. It is also comparable to those of the two C_4/C_6 architectures, error-correcting and postselecting ones [20].

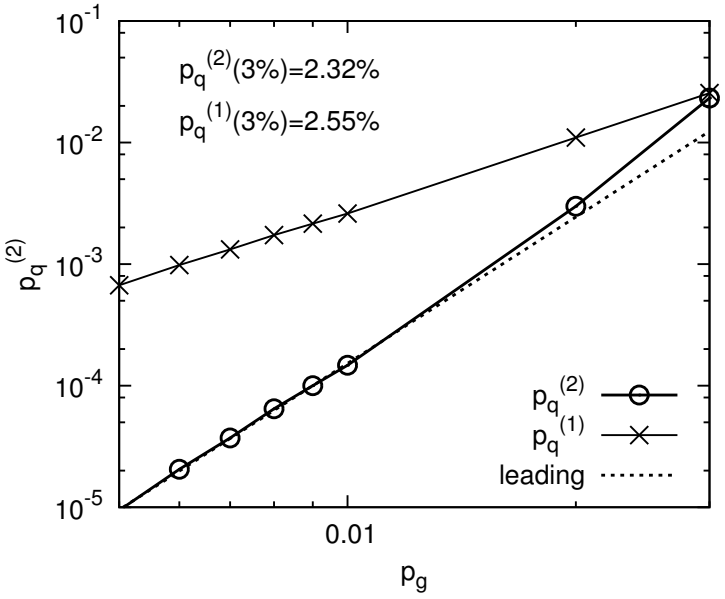


Figure 3.3: The error probability $p_q^{(2)}$ for measuring the level-2 qubit after the bare CZ connection is plotted as a function of the physical error probability p_g, together with the leading term ${}_7\mathrm{C}_2(p_q^{(1)})^2$ (dotted line). The upper-most line indicates $p_q^{(1)}$ in comparison to infer the threshold.

3.6 Resources usage

The physical resources (qubits and gates) are calculated by counting the numbers of hexaclusters, ancilla code states and bare CZ gates which are used in the diagrams for the construction of fundamental clusters. In this calculation we present recursion relations of the resources $R_\alpha^{(l)}$ required for the components $\alpha = S, D, h, 0, +$ corresponding to the single verification, double verification, hexacluster $|h\rangle$, ancilla qubits $|0\rangle$ and $|+\rangle$, respectively.

The single verification in the diagram (3.15) or its full version (3.16) uses 1×7 $|h^{(l)}\rangle$'s, 2 $|+^{(l)}\rangle$'s and 2 level-l transversal bare CZ gates, that is

$$R_S^{(l)} \;=\; 1\times 7R_h^{(l)} + 2(R_+^{(l)} + R_b^{(l)})(l \geq 2), \tag{3.43}$$

where

$$R_b^{(l)} = 7^l \tag{3.44}$$

indicates the resources for a level-l transversal bare CZ gate (the number of physical CZ gates). Similarly, the resources $R_D^{(l)}$ for the double verification, which uses 3×7 $|h^{(l)}\rangle$'s, 8 $|+^{(l)}\rangle$'s and $(8+2)$ level-l bare CZ gates in the diagram (3.18), are given as

$$R_D^{(l)} = 3\times 7R_h^{(l)} + 8(R_+^{(l)} + R_b^{(l)}) + 2R_b^{(l)}(l \geq 2). \tag{3.45}$$

Furthermore, the resources used to construct the level-$(l+1)$ fundamental clusters $|h^{(l+1)}\rangle$, $|0^{(l+1)}\rangle$ and $|+^{(l+1)}\rangle$ are counted from the reduced diagrams (3.20) and (3.21) as

$$R_\alpha^{(l+1)} = \sum_{\beta=S,D,0,b} \frac{n_\alpha^\beta R_\beta^{(l)}}{p_\alpha^{(l+1)}} (\alpha = h, 0, +; l \geq 1), \tag{3.46}$$

with the numbers of the respective level-l components

$$(n_h^S, n_h^D, n_h^0, n_h^b) = (2, 3, 6, 10), \tag{3.47}$$

$$(n_0^S, n_0^D, n_0^0, n_0^b) = (6, 7, 11, 26), \tag{3.48}$$

$$(n_+^S, n_+^D, n_+^0, n_+^b) = (5, 7, 10, 24), \tag{3.49}$$

and the success probabilities $p_\alpha^{(l+1)}$ for the clusters $|\alpha^{(l+1)}\rangle$ to pass the verification process with postselection. Here, the bare CZ gates are used in the processes, (i) the n_α^0 encodings with $|0^{(l)}\rangle$ ($\oplus$), and (ii) the $[2(n_\alpha^S + n_\alpha^D) - n_\alpha^0]$ connections between the outputs after the verifications and the inputs to the subsequent verifications, where n_α^0 is subtracted for the final outputs ($\circledcirc$). Thus, the number of the level-l bare CZ gates is given by $n_\alpha^b = 2(n_\alpha^S + n_\alpha^D)$, i.e., $n_h^b = 10$, $n_0^b = 26$ and $n_+^b = 24$. The bare CZ gates are also used in the verification diagrams, which are properly counted in $R_S^{(l)}$ and $R_D^{(l)}$. The level-1 resources are given in the circuits (3.14), (3.17) and (3.22) as

$$R_S^{(1)} = 3R_b^{(1)} + 2R_0^{(1)}, \tag{3.50}$$

$$R_D^{(1)} = 9R_b^{(1)} + 8R_0^{(1)}, \tag{3.51}$$

$$R_0^{(1)} = R_+^{(1)} = 69/p_0^{(1)}. \tag{3.52}$$

Here, $R_{0,+}^{(1)}$ is counted as follows. The Steane seven-qubit code state is encoded into 7 physical qubits by using 9 CNOT gates [100]. This code state is preliminarily verified through 3 stabilizer measurements, each of which consumes 1 ancilla qubit and 4 CNOT gates. At this stage $7 + 9 + 3 \times (1 + 4) = 31$ resources are used for each preliminarily verified code state. Then, the code sate is secondly verified according to the circuit (3.22), where 2 preliminarily verified code states and 7 (transversal) CNOT gates are used. Thus, the number of resources used to prepare the level-1 code state amounts to $R_{0,+}^{(1)} = (2 \times 31 + 7)/p_0^{(1)} = 69/p_0^{(1)}$ including the success probability $p_0^{(1)} = p_+^{(1)}$.

The success probabilities $p_\alpha^{(l)}$ have been evaluated in the numerical simulation for the cluster construction. In Fig. 3.4 we plot especially $p_0^{(l)}$ ($\leq p_+^{(l)} < p_h^{(l)}$) as functions of the physical error probability p_g for the levels $l = 1, 2, 3, 4$. The level-1 $p_\alpha^{(1)}$ appears to

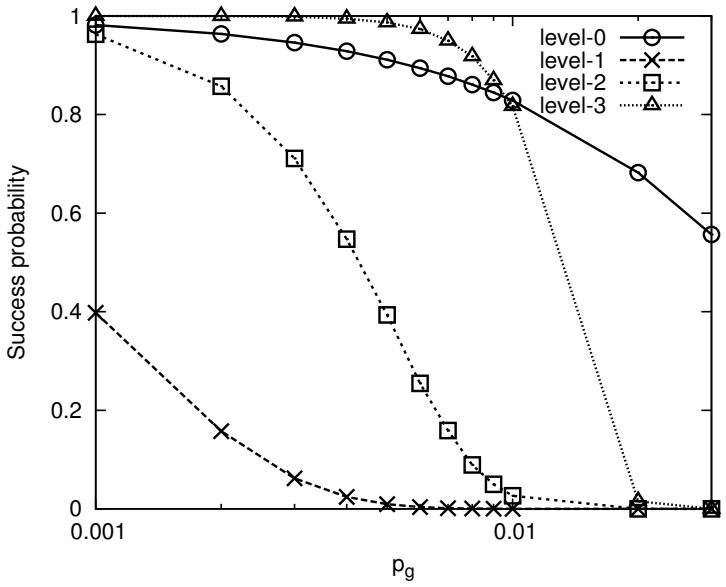


Figure 3.4: The success probabilities $p_0^{(l)}$ are plotted as functions of the physical error probability p_g for the levels $l = 1, 2, 3, 4$.

be rather high since the physical-level computation is implemented in the circuits with less operations. Then, the level-2 $p_\alpha^{(2)}$ decreases substantially due to the low fidelity of the level-2 fundamental clusters for the level-3 cluster construction. However, the success probabilities $p_\alpha^{(l)}$ almost approach unity at the level-4 and higher as the error probability $p_q^{(l)}$ for the logical qubit is reduced rapidly for $p_g < 1\%$ below the threshold.

The resources are evaluated by using the above recursion relations with the success probabilities $p_\alpha^{(l)}$ simulated numerically, depending on the computation size N, where the highest level is given as $\bar{l} \sim \log_2(\log_{10} N)$ to achieve the accuracy $0.1/N$. The results of $R_0^{(\bar{l})}$ ($> R_{h,+}^{(\bar{l})}$) are shown in Fig. 3.5 for the present architecture of verified logical clusters (LC) with $p_g = 10^{-2}$ and 10^{-3}, which are compared with the resources for the circuit-based Steane's QEC scheme with $p_g = 10^{-3}$ [19]. Each step in these graphs indicates the rise of the highest level $\bar{l}$ by one. We find that the present architecture really consumes much less resources than the Steane's QEC scheme for $p_g \leq 10^{-3}$ (checked numerically also for $p_g = 10^{-4}$). This indicates that the overhead costs paid for the verification process with postselection in the cluster construction are worth enough to save the total resources usage by reducing rapidly the logical error probability. Thus, the present cluster-based architecture is quite efficient with respect to both noise threshold and resources usage, compared with the usual circuit-based QEC schemes with the Steane seven-qubit code.

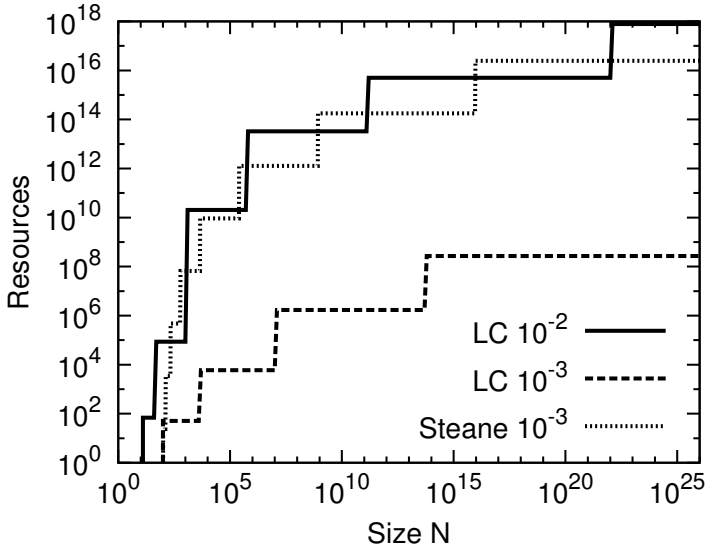


Figure 3.5: Resources for the present architecture of verified logical clusters (LC) with $p_g = 10^{-2}$ and 10^{-3}, which are compared with those for the Steane's QEC scheme with $p_g = 10^{-3}$.

We also compare the present architecture with the postselecting and error-correcting C_4/C_6 architectures [20]. The postselecting C_4/C_6 architecture makes use of the usual circuit-based nondeterminism for fault-tolerant gate operation, which is different from the error-precorrection in the cluster-based architecture. Thus, it requires for scalability the construction of a large QEC code state at a certain level with the decoding of the lower-level error-detection code, in order to implement the standard fault-tolerant computation at the higher levels. The resources usage of the postselecting C_4/C_6 architecture amounts to be large for the overhead cost of the large QEC code state. On the other hand, the noise threshold and resources usage for the error-correcting C_4/C_6 architecture with the Fibonacci scheme are both comparable to those for the present cluster-based architecture with the Steane seven-qubit code.

3.7 Miscellaneous

We further discuss some issues concerning the performance of the cluster-based architecture.

3.7.1 Memory error effect

The memory errors may be significant in the cluster-based architecture without recovery operation. The qubits to form the clusters are not touched directly (but via one-bit teleportation) through the concatenated constructions after the level-1 verification. Then, the memory errors accumulate until they are measured in the upper-level construction. The memory errors are added as $p_q^{(0)} + \bar{l}(n\tau_m p_g)$, where $\tau_m p_g$ denotes the probability of memory error with the effective waiting time τ_m for one measurement, and n is the number of waiting time steps at each concatenation level (e.g., $n = 12$ for the hexacluster). The noise threshold is thus estimated roughly as

$$p_{\rm th} \sim [{}_7{\rm C}_2\{1 + \log_2(\log_{10} N)n\tau_m\}]^{-1}, \tag{3.53}$$

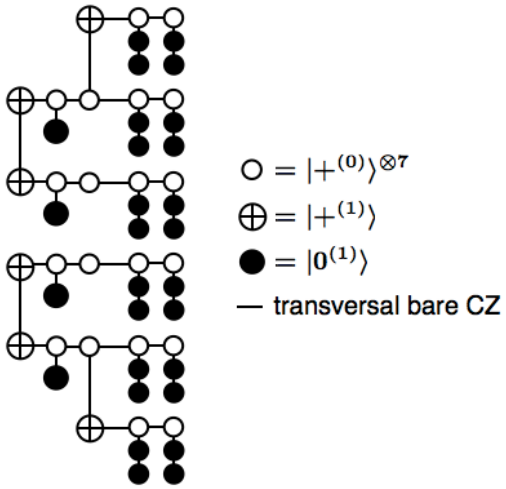
depending on the computation size N with the highest level $\bar{l} \sim \log_2(\log_{10} N)$. For example, $p_{\rm th} \sim 1\%$ for $N \sim 10^{20}$ and $\tau_m = 0.1$ ($n \sim 10$), which will be tolerable for practical computations.

It seems difficult to surmount essentially the problem of memory error in the present framework. As a partial resolution for the memory error accumulation, the fundamental clusters as two-colorable graph states may be refreshed at the first one or two logical levels by using a purification protocol [86, 87, 109]. This process will relax the deterioration of the noise threshold to some extent though it requires a significant overhead cost. However, the purification at the higher levels are not realistic since the success probability of purification drops exponentially with the increasing number of physical qubits in the logical clusters.

3.7.2 One-way computation at the physical level

We may use the one-way computation even at the physical level, instead of the circuit computation, for the construction of level-2 fundamental clusters. The level-1 qubits are encoded through the verification by the cluster versions of the circuits in (3.22). Then, the level-2 hexa cluster is constructed through the single and double verifications as given in the reduced diagram in (3.20) by combining the physical qubits and level-1 code states

with the transversal bare CZ gates:



(3.54)

The level-2 code states are constructed similarly according to the reduced diagrams in (3.21). The homogeneous errors for the resultant level-1 qubits (components of the level-2 clusters) are estimated in the first order by inspecting the double verification process in the final stage, where extra CZ gates are required for the CNOT gate operations inducing additional errors: $\epsilon_X = p_{XI}$, $\epsilon_Y = p_{YI}$, $\epsilon_Z = p_p + p_{XZ} + p_{IZ} + p_{ZY} + p_{YY} + p_{ZI} + p_{ZI}$. The noise threshold is slightly lowered as $p_{\rm th} \simeq 0.03$ with $D = 5/3$ in Eq. (3.42).

3.7.3 Application of other QEC codes

So far we have considered only the Steane seven-qubit code in the present architecture. Here, we briefly discuss application of some other QEC codes, say code C. If the code C is a self-dual CSS code or a CSS code which has high symmetry such as the Bacon-Shor subsystem code, the cluster-based architecture can be applied straightforwardly by taking the hexacluster and the graph state equivalents of the code states of C as the fundamental clusters. The behavior of logical errors is, however, somewhat different, depending on the distance of C as seen in the following two examples.

We first consider the four-qubit error detection code C_4. The Fibonacci scheme can be used for the C_4 code to generate deterministically the logical measurement outcomes from the physical ones in one-way computation. Then, the cluster-based concatenation can be carried out with the error detection code C_4 almost in the same way as with the Steane seven-qubit code. In this case, we may reduce the resources to prepare the level-2 fundamental clusters with high success probability, since the number of error locations

is smaller than that for the Steane seven-qubit code [20, 21, 23, 24]. As a trade-off the error probability for the Pauli frame becomes $p^{(1)}_{\rm Pauli} \sim p_g^3$, while the error probability for measuring the level-1 qubit is $p_q^{(1)} \sim p_g^2$. Thus, the Pauli frame provides a more significant error contribution near the threshold than the case of the Steane seven-qubit code with $p^{(1)}_{\rm Pauli} \sim p_g^4$.

We next consider the Golay code, which is a 23-qubit self-dual CSS code with distance 7. In this case, although we have to pay much more resources at the lowest level, the logical errors are reduced substantially as $p_q^{(1)} \sim p_g^4$ and $p^{(1)}_{\rm Pauli} \sim p_g^8$ [19, 89]. Thus, it will be possible to improve the noise threshold of the cluster-based architecture by using the Golay code.

We further mention that even with the Steane seven-qubit code the present architecture has a room to improve its performance. The optimal decoding (adaptive concatenation) technique [110, 111], which boosts the correctable error of the Steane seven-qubit code up to $\sim$ 11%, is readily available to improve the noise threshold by generating efficiently the logical measurement outcomes in one-way computation.

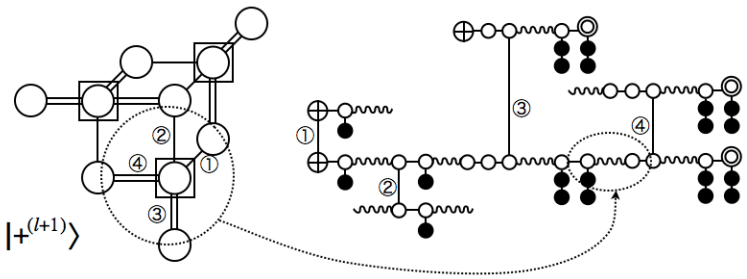
3.8 Conclusion

We have investigated an efficient architecture for fault-tolerant quantum computation, which is based on the cluster model of encoded qubits. Some relevant logical cluster states, fundamental clusters, are constructed through verification without recovery operation in concatenation, which provides the error-precorrection of gate operations for the one-way computation at the higher level. A suitable code such as the Steane seven-qubit code is adopted for transversal operations. This construction of fundamental clusters provides a simple transversal structure of logical errors in concatenation, and achieves a high noise threshold by using appropriate verification protocols, namely the single and double verifications. Since the postselection is localized within each fundamental cluster with the help of deterministic bare CZ gates without verification, divergence of resources is restrained, which reconciles postselection with scalability. Detailed numerical simulations have really confirmed these desired features of the cluster-based architecture. Specifically, the noise threshold is estimated to be about 3%, and the resources usage is much less than those of the usual circuit-based QEC schemes with the Steane seven-qubit code. This performance is comparable to that of the error-correcting C_4/C_6 architecture with the

Fibonacci scheme. Some means may hopefully be applied for the cluster-based architecture to improve its performance, including the error-detecting C_4 code with the Fibonacci scheme, other self-dual CSS codes such as the Golay code, which are more robust for logical encoding than the Steane seven-qubit code, and the adoptive concatenation or optimal decoding.

Appendix A
Diagrams for cluster construction

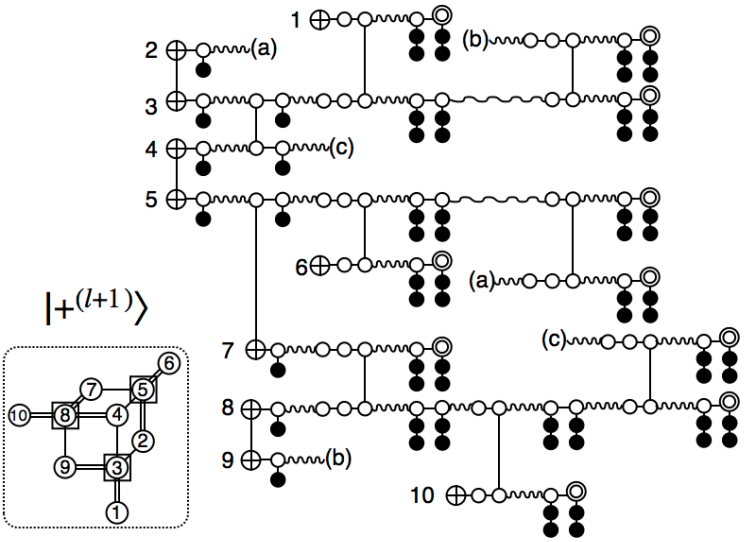
We can produce systematically the diagrams for cluster construction from the reduced ones (3.20) and (3.21), according to the following rules: (i) Replace the single edge with the single verification (3.15). (ii) Replace the double edge with the double verification (3.18) so that the double verifications are always placed at the right side (namely later in time) of the single verifications. (iii) Put the $\oplus$ encodings on the input qubits at the leftmost (initially in time). (iv) Apply the bare CZ gate (wavy line) to connect the output qubit of the preceding verification to the input qubit of the following verification. In the case that the double verification is followed by the other double verification, we cut off the leftmost qubit of the following verification by measurement before connecting these double verifications, in order to remove the redundant H rotation. This prescription is illustrated in the following diagram:



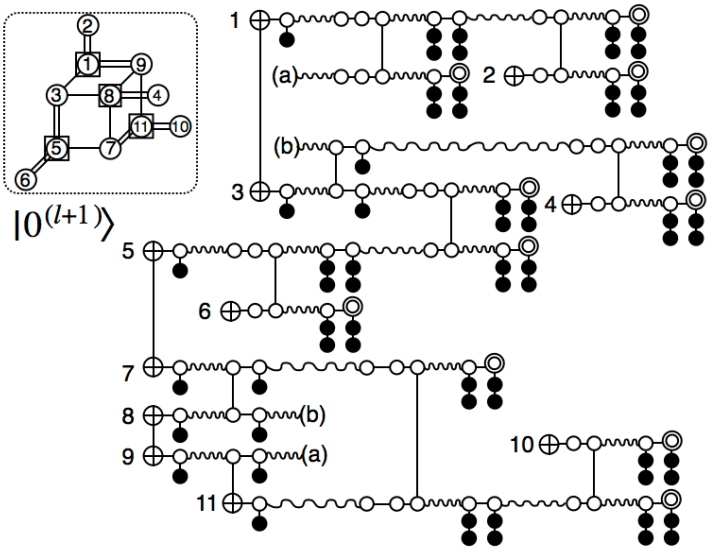
(3.55)

The cluster diagram (3.19) for $|h^{(l+1)}\rangle$ is generated according to these rules (i)–(iv). The cluster states for $|+^{(l+1)}\rangle$ and $|0^{(l+1)}\rangle$ are constructed similarly in the following diagrams, where the pairs of the same characters such as (a)-(a) are actually connected by the bare

CZ gates:



(3.56)



(3.57)

Chapter 4

Entanglement purification with double selection

In this chapter, we investigate an entanglement purification protocol with double selection process, which works under imperfect local operations. Compared with the usual protocol with single selection, this double-selection method has higher noise thresholds for the local operations and quantum communication channels, and achieves higher fidelity of purified states. It also provides a yield comparable to that of the usual protocol with single selection. We discuss on general grounds how some of the errors which are introduced by local operations are left as intrinsically undetectable. The undetectable errors place a general upper bound on the purification fidelity. The double selection is a simple method to remove all the detectable errors in the first order so that the upper bound on the fidelity is achieved in the low noise regime. The double selection is further applied to purification of multipartite entanglement such as two-colorable graph states.

4.1 Introduction

Recently a number of protocols based on entanglement have been developed in quantum communication and computation. For example, bipartite entanglement is employed in quantum teleportation, superdense coding, quantum cryptography and quantum repeater [37, 112, 113, 114, 115]. Multipartite entanglement is further utilized in cluster state computation, quantum error correction and multiparty cryptography [11, 41, 42, 45]. The performance of these entanglement-based protocols highly depends on the fidelity of entangled states. That is, high fidelity entangled states are essential for secure communication and reliable computation. In this viewpoint, it is a very important task to prepare

and share high fidelity entangled states.

Entanglement purification is a way to share high fidelity entangled states via noisy communication channels. It was proposed originally to share Einstein-Podolsky-Rosen (EPR) states [77, 116, 117], and then extended for a large class of multipartite entangled states, including the Greenberger-Horne- Zeilinger (GHZ) states, two-colorable graph states, stabilizer states and W states [86, 87, 118, 119, 120, 121, 122, 123]. In a situation with noisy channels but perfect local operations, one may pre-purify initial states with a recurrence protocol, which has a high threshold for the noise of the communication channel but gives a low yield of purified states. Then, a hashing protocol may be implemented to get pure entangled states with a nonzero yield. The hashing protocol, however, breaks down as soon as local operations become slightly imperfect [119]. The entanglement purification under imperfect local operations was first analyzed in the context of quantum repeater [114, 115], where the usual recurrence protocol [77, 116, 117] is adopted. The fidelity of purified states is indeed limited by the imperfection of local operations, and noise thresholds exist for successful purification. This is clearly distinct from the cases such as a hashing protocol where perfect local operations are assumed. One should confront the problem that errors are introduced inevitably by local operations themselves for purification even if the initial impurity is diminished. Thus, in order to realize entanglement-based protocols by using practical devices, which inevitably have imperfections, we need to develop purification methods which work well with noisy local operations.

In this chapter we investigate an entanglement purification protocol with more accurate postselection through double verification process, which works under imperfect local operations. Compared with the usual protocol with single selection [77, 114, 115, 116, 117], this double-selection method has higher noise thresholds for the local operations and communication channels, and achieves higher fidelity of purified states. It can be shown on general grounds how some of the errors which are introduced by local operations are left as intrinsically undetectable. This limitation on the achievable fidelity due to the undetectable errors is applicable to a wide variety of purification protocols [77, 86, 87, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124]. The double selection is indeed a simple method to remove all the detectable errors in the first order so that in the low noise regime the purification fidelity reaches the general upper bound which is placed by the undetectable errors. It may be considered that the elaborate postse-

lection decreases the yield of purification by consuming many resources. However, this is not necessarily the case. The double-selection protocol provides a yield comparable to or even better than that of the single-selection protocol. This is because the double selection increases the fidelity faster by removing more errors in each purification round. The double selection is also applicable to purification of multipartite entanglement such as two-colorable graph states [86, 87, 119].

The rest of the chapter is organized as follows. In Sec. 4.2 we investigate the double selection in the bipartite entanglement purification. The performance of the double-selection protocol is analyzed and compared with that of the usual protocol with single selection. In Sec. 4.3 the upper bound on the fidelity is discussed in terms of the intrinsically undetectable errors which are introduced by local operations. This bound is really achieved by the double-selection protocol in the low noise regime. In Sec. 4.4 the double selection is applied to the multipartite entanglement purification, where the Steane seven-qubit code is investigated as an example of two-colorable graph states. Section 4.5 is devoted to conclusion. Detailed calculations of the transition probability tensors to characterize the purification maps are presented in Appendix B.

4.2 Bipartite entanglement purification

4.2.1 Single selection

We first review the usual recurrence protocol for purification where the single selection is made [77, 116, 117]. This protocol is implemented by using two noisy copies of an EPR pair, a bilateral CNOT gate and a bilateral measurement in each round of purification. Here, a bilateral operation means a tensor product of two identical local operations which are simultaneously implemented by the two parties, Alice and Bob. The purification procedure is specifically described as follows (see Fig. 4.1):

(i) Alice and Bob share two identical EPR pairs $\rho^{(0)}$ and $\rho^{(1)}$ through a noisy quantum channel.

(ii) They operate a bilateral CNOT gate on $\rho^{(0)}$ and $\rho^{(1)}$ as the control and target qubits, respectively.

(iii) They bilaterally measure $\rho^{(1)}$ in the Z basis $\{|0\rangle, |1\rangle\}$, and obtain the measurement outcomes m_a (Alice) and m_b (Bob).

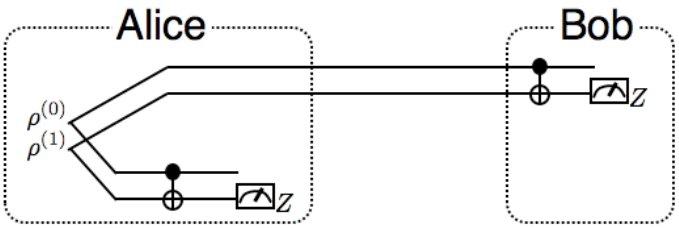


Figure 4.1: Bipartite entanglement purification with single selection.

(iv) They keep $\rho^{(0)}$ if the measurement outcomes coincide as $m_a = m_b$. Otherwise, they discard $\rho^{(0)}$.

A single bilateral operation determines whether $\rho^{(0)}$ should be kept or discarded, namely the single selection. Alice and Bob iterate procedures (ii)–(iv) by using the output states which survive the selection in procedure (iv) as the input states for the next round of purification where the direction (control and target) of the bilateral CNOT gate is inverted, and the measurement is made in the X basis (Oxford protocol) [117]. This inversion round by round may be done mathematically by applying a Hadamard transformation (perfect by itself) on each qubit to exchange the bases of the reference frame as $X \leftrightarrow Z$.

The noisy EPR pairs $\rho^{(0)}$ and $\rho^{(1)}$ are given as two copies of a Bell-diagonal state ρ,

$$\rho^{(0)} = \rho^{(1)} = \rho = \sum_{i=0}^{3} F_i \phi_i, \tag{4.1}$$

where the Bell states are

$$\phi_i \equiv |\phi_i\rangle\langle\phi_i|, \tag{4.2}$$

$$|\phi_i\rangle = \sigma_i \otimes \sigma_0(|00\rangle + |11\rangle)/\sqrt{2} \tag{4.3}$$

with $\sigma_0 = I$ and the Pauli operators σ_i $(i = 1, 2, 3)$. In the rest of this chapter, we simply use the term "EPR pair" to denote a noisy EPR pair as a Bell-diagonal mixed state, which passes through some noisy quantum communication channel and purification procedure. The above purification procedure generates a transformation of the input Bell-diagonal ρ with the state-vector $\mathbf{F} = (F_0, F_1, F_2, F_3)$ to another Bell-diagonal ρ' with the state-vector $\mathbf{F}' = (F'_0, F'_1, F'_2, F'_3)$, even when the Pauli noise is introduced for the local operations. The imperfect CNOT gate, which is operated locally by Alice, is described as

a sequence of a perfect CNOT gate operation $\mathcal{U}$ and a two-qubit deporalizing noise with error probabilities p_{ij} as

$$\mathcal{N}(\rho_{\mathcal{U}}^{(0,1)}) = \sum_{ij} p_{ij}(\sigma_i \otimes \sigma_j)_A \otimes \mathbf{1}_B \rho_{\mathcal{U}}^{(0,1)} (\sigma_i \otimes \sigma_j)_A \otimes \mathbf{1}_B, \tag{4.4}$$

where $\rho_{\mathcal{U}}^{(0,1)} = \mathcal{U}(\rho^{(0)} \otimes \rho^{(1)})$, $p_{00} = 1 - p_g$ with $p_g = \sum_{ij \neq 00} p_{ij}$, the Pauli operators $(\sigma_i \otimes \sigma_j)_A$ act on the control and target qubits at Alice, respectively, and $\mathbf{1}_B$ indicates the identity operator acting on the qubits at Bob. The imperfect CNOT gate operated by Bob is described in the same manner. The imperfect measurement of a qubit in the Z basis is described by positive-operator-valued measure (POVM) elements with an error probability p_m as

$$E_0 = (1 - p_m)|0\rangle\langle 0| + p_m|1\rangle\langle 1|, \tag{4.5}$$

$$E_1 = (1 - p_m)|1\rangle\langle 1| + p_m|0\rangle\langle 0|. \tag{4.6}$$

The X measurement is also described by $E_+ = HE_0H$ and $E_- = HE_1H$ with a Hadamard transformation H.

Given these imperfect operations, the purification map in the R^4 space

$$\mathbf{F}' = \mathcal{S}(\mathbf{F}) \tag{4.7}$$

is described specifically [114, 115, 117] as

$$F_i' = \frac{1}{p_S(\mathbf{F})} \sum_{jk} S_i^{jk}(p_{ab}, p_m) F_j F_k, \tag{4.8}$$

where

$$p_{\mathcal{S}}(\mathbf{F}) = \sum_{ijk} S_i^{jk}(p_{ab}, p_m) F_j F_k \tag{4.9}$$

is the success probability responsible for the normalization $\sum_i F_i' = 1$. The transition probability tensor $S_i^{jk}(p_{ab}, p_m)$ is calculated in Appendix B including the error probabilities of a CNOT gate (p_{ab}) and a measurement (p_m). The maximum achievable fidelity of purified states is determined by iterating the purification map.

4.2.2 Double selection

The double-selection protocol is implemented by using three noisy copies of an EPR pair, two bilateral CNOT gates and two bilateral measurements in each round of purification, as described in the following (see Fig. 4.2):

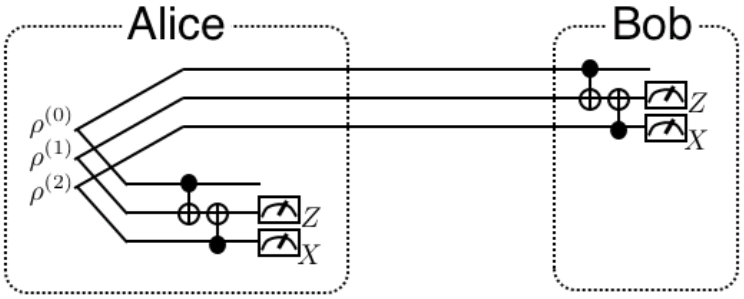


Figure 4.2: Bipartite entanglement purification with double selection.

(i) Alice and Bob share three identical EPR pairs $\rho^{(0)}$, $\rho^{(1)}$ and $\rho^{(2)}$ through a noisy quantum channel.

(ii) They operate a bilateral CNOT gate on $\rho^{(0)}$ and $\rho^{(1)}$ as the control and target qubits, respectively.

(iii) Next they operate a bilateral CNOT gate on $\rho^{(2)}$ and $\rho^{(1)}$ as the control and target qubits, respectively.

(iv) They bilaterally measure $\rho^{(1)}$ and $\rho^{(2)}$ in the Z and X bases, respectively, and obtain the measurement outcomes $m_a^{(1)}$, $m_a^{(2)}$ (Alice) and $m_b^{(1)}$, $m_b^{(2)}$ (Bob).

(v) They keep $\rho^{(0)}$ if the outcomes coincide for both of the measurements as $m_a^{(1)} = m_b^{(1)}$ and $m_a^{(2)} = m_b^{(2)}$. Otherwise, they discard $\rho^{(0)}$.

Similarly to the single-selection protocol, Alice and Bob iterate procedures (ii)–(v) by using the output states which survive the selection in procedure (v) as the input states for the next round where the X and Z bases of their reference frames are exchanged by a Hadamard transformation.

The above procedure provides a purification map

$$\mathbf{F}' = \mathcal{D}(\mathbf{F}), \tag{4.10}$$

which is given by cubic combinations of the initial-state components in the case of double selection as

$$F_i' = \frac{1}{p_{\mathcal{D}}(\mathbf{F})} \sum_{jkl} D_i^{jkl}(p_{ab}, p_m) F_j F_k F_l, \tag{4.11}$$

where

$$p_{\mathcal{D}}(\mathbf{F}) = \sum_{ijkl} D_i^{jkl}(p_{ab}, p_m) F_j F_k F_l. \tag{4.12}$$

The transition probability tensor $D_i^{jkl}(p_{ab}, p_m)$ is calculated in Appendix B.

The double selection by the elaborate error detection with two ancilla EPR pairs can remove errors more efficiently than the single selection, as will be explained in Sec. 4.3. This improves significantly the achievable fidelity and the noise threshold. Here, it should be mentioned that the purification protocol for large two-colorable graph states [119] also uses three copies of a state and two multi-lateral CNOT gates. In spite of this apparent similarity, the protocol of Ref. [119] is essentially different from the present double selection. In the double selection of Fig. 4.2 the source state $\rho^{(0)}$ is connected with the first ancilla $\rho^{(1)}$, and the first ancilla $\rho^{(1)}$ with the second ancilla $\rho^{(2)}$ for the optimal error detection and postselection. On the other hand, in the protocol of Ref. [119] both of the two ancilla states are connected with the source state by the CNOT gates in the same direction. This setup is adopted for the error correction to provide deterministically one purified state from three copies, which is efficient for the yield of purification. It, however, cannot remove fully the detectable errors, providing even lower fidelity than the single-selection protocol (see also a discussion in Sec. 4.3). Generally, protocols based on postselection provide high fidelities and high noise thresholds, but exponentially diminishing yields as the size of purified state increases. Here, we aim to purify entangled states of relatively small size such as the EPR pair and Steane seven-qubit code state, achieving a high fidelity and a high noise threshold with a tolerable yield.

4.2.3 Performance analysis

We now compare the single and the double selections in performance by considering the minimum fidelity required for the quantum communication channel, the maximum achievable fidelity of purified states, the working range for the noise of local operations, and the EPR resources consumed to achieve a target fidelity.

The EPR pairs of ϕ_0 are shared initially through a noisy communication channel $\mathcal{C}$ as

$$\mathcal{C}(\rho) = F_{\rm ch}\rho + \sum_{i=1}^{3} r_i \epsilon_{\rm ch} \sigma_i \otimes \sigma_0 \rho \sigma_i \otimes \sigma_0, \tag{4.13}$$

where $F_{\rm ch}$ and $r_i\epsilon_{\rm ch}$ with $\epsilon_{\rm ch} \equiv 1 - F_{\rm ch}$ and $\sum_{i=1}^{3} r_i = 1$ represent the channel fidelity and error probabilities, respectively. Then, the purification is started for a Bell-diagonal state

$\mathcal{C}(\phi_0)$ as a noisy EPR pair with the state-vector

$$\mathbf{F}^{(0)} = (F_{\rm ch}, r_1\epsilon_{\rm ch}, r_2\epsilon_{\rm ch}, r_3\epsilon_{\rm ch})\,. \tag{4.14}$$

By operating the purification map $\mathcal{A}$ ($\mathcal{S}$ or $\mathcal{D}$) recursively, the state-vector $\mathbf{F}^{(n)}$ after the nth round is given by

$$\mathbf{F}^{(n)} \;=\; \mathcal{A}(\mathbf{F}^{(n-1)}). \tag{4.15}$$

The behavior of the Bell-diagonal states through the purification rounds is as follows. First, suppose that the errors of local operations are sufficiently small, that is, inside the working range. Then, if the initial fidelity $F_0^{(0)} = F_{\rm ch}$ is higher than some threshold value $F_{\rm min}$ (the minimum required fidelity), the state-vector $\mathbf{F}^{(n)}$ approaches a fixed point in R^4 with a fidelity $F_{\rm max}$ (the maximum achievable fidelity), which is higher than $F_{\rm ch}$ ($> F_{\rm min}$). On the other hand, if $F_{\rm ch} < F_{\rm min}$, $\mathbf{F}^{(n)}$ goes to another fixed point $\mathbf{F}_{\rm mix} = (1/4, 1/4, 1/4, 1/4)$ representing the completely mixed state. Next, if the errors are outside the working range, the purification map no longer admits the fixed point for $F_{\rm max}$. Then, irrespective of the value of $F_{\rm ch}$, $\mathbf{F}^{(n)}$ goes to $\mathbf{F}_{\rm mix}$, that is, the purification turns out to be impossible. We have checked these behaviors by numerical calculations. The values of the initial fidelity and error parameters have been taken by scanning over $1/4 \le F_{\rm ch} < 1$ and $0 \le p_g, p_m < 0.3$, where $p_{ij} = p_g/15$ ($ij \neq 00$) and $p_{00} = 1 - p_g$ are adopted typically for the CNOT gate errors. Then, by tracing the transition of the Bell-diagonal states round by round according to the purification map, $F_{\rm min}$, $F_{\rm max}$, and the working range have been determined numerically, as done in the preceding study for the protocol with single selection [114, 115]. Here, as in the Oxford protocol [117], the twirling operation to depolarize Bell-diagonal states to Werner states is not made in each round, since the twirling with imperfect operations really lowers the achievable fidelity [114, 115].

In the following, we show the results of numerical calculations on the performance of the present protocol, where a Werner state with $r_i = 1/3$ is taken initially in Eq. (4.14) as a typical case. Similar results are obtained for general Bell-diagonal states with various r_i, as discussed later.

In Fig. 4.3, $F_{\rm max}$ (upper curves) and $F_{\rm min}$ (lower curves) are plotted as functions of the error probability p, where $p = p_g = p_m$ are taken for definiteness. The double selection clearly achieves higher fidelity $F_{\rm max}$ with lower minimum required channel fidelity $F_{\rm min}$, compared with the single selection (Oxford protocol [114, 115, 117]). The working range of

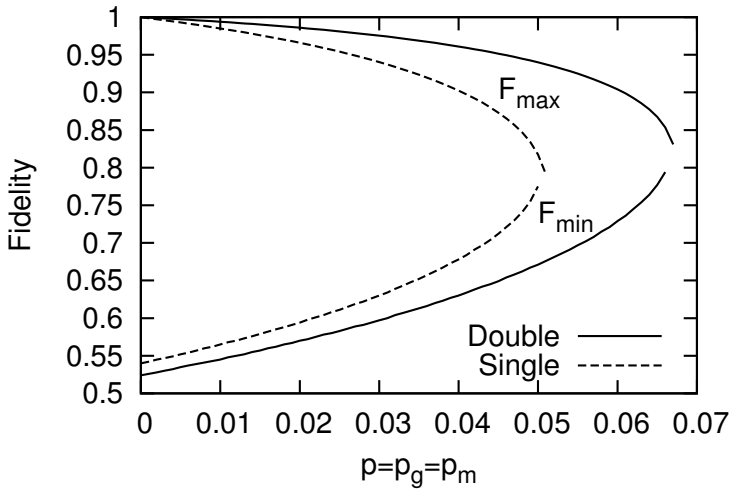


Figure 4.3: Maximum achievable fidelity $F_{\max}$ (upper curves) and minimum required channel fidelity $F_{\min}$ (lower curves) are plotted as functions of the error probability $p = p_g = p_m$ for the double and single selections.

(p_g, p_m) is shown in Fig. 4.4. The purification is implemented successfully for $F_{\rm ch} > F_{\min}$ to achieve $F_{\max}$, if (p_g, p_m) is below each threshold curve. (The point on the threshold curve for $p = p_g = p_m$ really corresponds to the intersection point of the curves of $F_{\min}$ and $F_{\max}$ in Fig. 4.3.) It is found that the double-selection scheme has higher thresholds (the wider working range) for the errors of local operations than the single-selection scheme. We may also take $p_{i0} = p_{0i} = q_i$ and $p_{ij} = q_i q_j$ $(i, j \neq 0)$ for the error parameters, as adopted in Ref. [125]. Then, we estimate the threshold values 3.7% and 4.2% of p_g $(q_i = p_g/3)$ with $p_m = 0$ for the single and double selections, respectively. The threshold value for the double selection is closer to an upper bound 5.3%, which is derived under some reasonable assumptions in Ref. [125]. The real bound would be located around 5% although it is outside our scope to determine it.

Here, we mention that the same achievable fidelity $F_{\max}$ is obtained even if general Bell-diagonal states with various r_i in Eq. (4.14) are taken initially. This is because $F_{\max}$ is given as the fixed point of the purification map, which is characterized by the local operations independently of the initial Bell-diagonal state. On the other hand, the minimum required channel fidelity $F_{\min}$ and the working range of (p_g, p_m) depend slightly on the choice of initial state. We have confirmed these features numerically by sampling the initial Bell-diagonal states with various r_i.

We next compare the yields of the two purification protocols. In the purification with

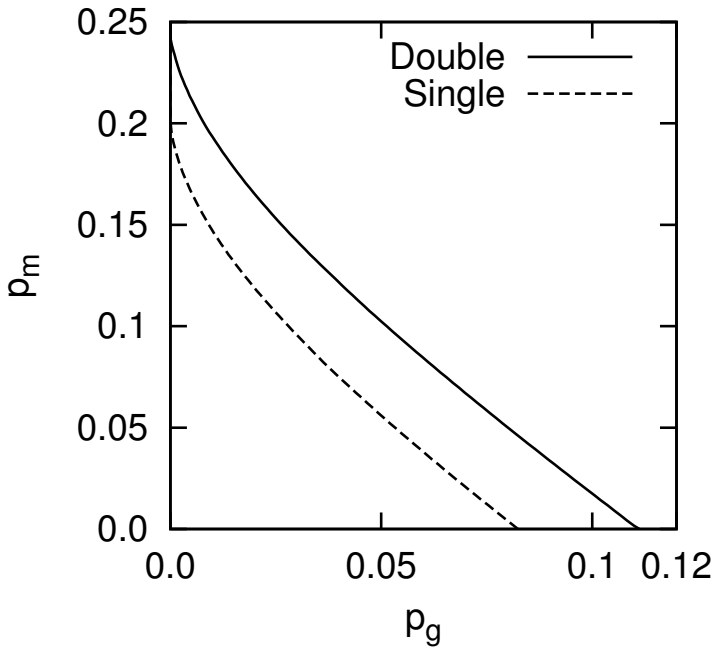


Figure 4.4: Working range (p_g, p_m) of local operations. Each purification protocol $\mathcal{A}$ ($\mathcal{S}$ or $\mathcal{D}$) achieves $F_{\max}$ for $F_{\rm ch} > F_{\min}$ when the error probabilities p_g and p_m are below the threshold curve (solid line for $\mathcal{D}$ and dotted line for $\mathcal{S}$).

imperfect local operations, the yield $Y_{\mathcal{A}}(F, F_{\rm ch})$ is defined as the inverse of the number of EPR pairs consumed to achieve a target fidelity F (< 1) under the channel fidelity $F_{\rm ch}$ [122]. It is calculated for each protocol $\mathcal{A} = \mathcal{S}, \mathcal{D}$ as

$$Y_{\mathcal{A}}(F, F_{\rm ch}) = \left[\prod_{n=1}^{n_{\mathcal{A}}(F,F_{\rm ch})} N_{\mathcal{A}}/p_{\mathcal{A}}(\mathbf{F}^{(n-1)}) \right]^{-1}, \tag{4.16}$$

where $n_{\mathcal{A}}(F, F_{\rm ch})$ denotes the minimum number of rounds, which is required to achieve the fidelity F; $p_{\mathcal{A}}(\mathbf{F}^{(n-1)})$ denotes the probability to pass the purification procedure in the nth round, as given in Eqs. (4.9) and (4.12); and $N_{\mathcal{A}}$ denotes the number of EPR pairs consumed in each round ($N_{\mathcal{S}} = 2$ and $N_{\mathcal{D}} = 3$).

We plot in Fig. 4.5 the yield $Y_{\mathcal{A}}(F, F_{\rm ch} = 0.8)$ as a function of the target fidelity F for each protocol with $p_g = p_m = 0.02$ (upper curves) and $p_g = p_m = 0.04$ (lower curves). By using less noisy local operations with $p_g = p_m = 0.02$, both protocols provide comparable yields to achieve $F \approx 0.9$, where the numbers of purification rounds are $n_{\mathcal{S}} = 4$ (single) and $n_{\mathcal{D}} = 2$ (double), respectively. On the other hand, even when noisier local operations with $p_g = p_m = 0.04$ are used, the double-selection protocol still provides a reasonable

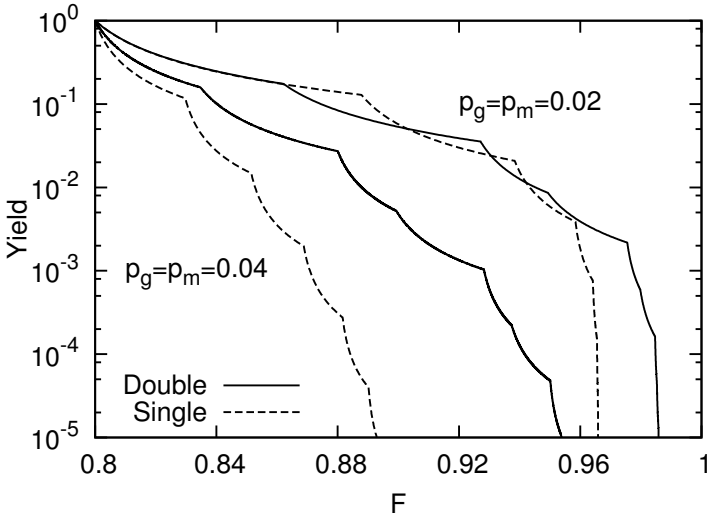


Figure 4.5: The yield $Y_{\mathcal{A}}(F, F_{\rm ch} = 0.8)$ is plotted as a function of the target fidelity F for each protocol with $p_g = p_m = 0.02$ (upper curves) and $p_g = p_m = 0.04$ (lower curves).

yield to achieve $F \approx 0.9$, where $n_{\mathcal{S}} = 16$ and $n_{\mathcal{D}} = 4$. Since the double selection uses three EPR pairs in each round, it may be thought to cost more resources than the single selection with two EPR pairs in each round. However, as seen in the above, the double selection provides a comparable or even better yield. This is because, by making the optimal error detection with two ancilla EPR pairs, the double selection can increase the fidelity of the source EPR pair considerably faster than the single selection, which will be discussed in the next section.

4.3 Purification fidelity limited by undetectable errors

Here we discuss on general grounds how the errors of local operations limit the fidelity of purified states. Specifically, it is shown that some of the errors introduced by the gate operations in the final stage of purification are left as intrinsically undetectable. The double selection is indeed a simple method to remove all the detectable errors, other than the intrinsically undetectable ones, in the first order. Thus, in the low noise regime it achieves the general upper bound on the purification fidelity which is placed by the undetectable errors.

The final stage of any protocol of bipartite entanglement purification may be viewed as the combination of two bilateral CNOT gates, as shown in Fig. 4.6, or its variants as

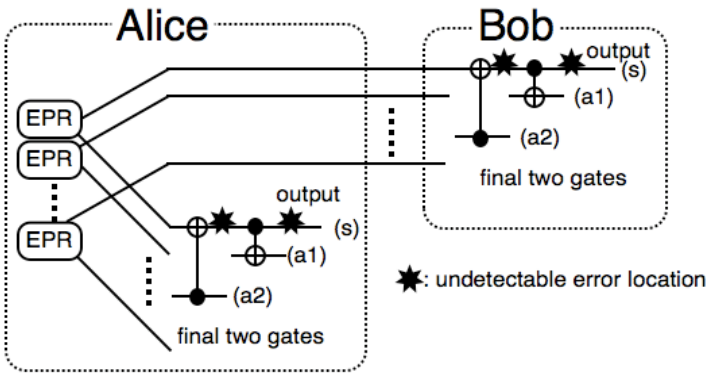


Figure 4.6: Setup of a protocol of bipartite entanglement purification. An upper bound on the fidelity is determined in the first order by the undetectable errors (indicated by black stars) introduced by the final two CNOT gates. Similar bounds are obtained with other configurations of two-qubit gates.

considered later. We inspect these final CNOT gate operations in Alice's site to observe the undetectable errors which are left on the output source qubit (s). (The same argument is made in Bob's site.) Passing through the final two gates, the preceding $\sigma_i^{(\mathrm{s})}$ errors ($i = 1, 2, 3$) on the source qubit (s) are propagated to either or both of the ancilla qubits (a1) and (a2). [It is possible that (a1) $\equiv$ (a2).] Thus these preceding errors are all detectable, and they can be removed by postselection after measuring the ancilla EPR pairs (a1) and (a2) in some appropriate way. The fidelity is limited ultimately by some of the errors introduced by the final two gates themselves (black stars in Fig. 4.6), which are *intrinsically undetectable without leaving any information on the ancillae*. As for the errors of the second-to-final CNOT gate, the $\sigma_3^{(\mathrm{s})} \otimes \sigma_0^{(\mathrm{a2})}$ error with the probability p_{30} is undetectable, since $\sigma_3^{(\mathrm{s})}$ is not propagated to ancilla (a1), commuting with the final CNOT gate. The $\sigma_{1,2}^{(\mathrm{s})} \otimes \sigma_0^{(\mathrm{a2})}$ (through the final CNOT gate) and $\sigma_i^{(\mathrm{s})} \otimes \sigma_j^{(\mathrm{a2})}$ errors, on the other hand, affect ancillae (a1) and (a2), respectively, and thus they are detectable. The $\sigma_i^{(\mathrm{s})} \otimes \sigma_0^{(\mathrm{a1})}$ errors of the final CNOT gate with the probabilities p_{i0} are also undetectable, since the output source (s) does not interact with any other ancillae afterward (by definition of the "final" CNOT gate). By subtracting the probabilities of these undetectable and thus irremovable errors at each party, an upper bound on the fidelity is placed in the first order as

$$F_{\mathrm{upper}} = 1 - N \left(p_{30} + \sum_{i=1}^{3} p_{i0} \right), \tag{4.17}$$

where $N = 2$ (Alice and Bob) for bipartite entanglement purification. Similar arguments

are made for N-partite entanglement purification to derive this upper bound. Note that the measurement error is not involved in Eq. (4.17). A portion of the component of the right state ϕ_0 may be discarded due to the errors in measuring the ancillae for verification. This slight reduction in the right state is, however, cancelled in the first order by the renormalization after the postselection. The gate errors $\sigma_0^{(\mathrm{s})} \otimes \sigma_j^{(\mathrm{a1})}$ and $\sigma_0^{(\mathrm{s})} \otimes \sigma_j^{(\mathrm{a2})}$, which affect only the ancillae, do not contribute either to F_{upper} in the first order by the same reason as the measurement errors.

In another protocol the final two CNOT gates may be exchanged in Fig. 4.6. (This is actually the case in the recurrence protocols considered in Sec. 4.2 when the purification procedure is finished at an even round.) Similarly, by observing the undetectable errors, we obtain an upper bound on the fidelity as

$$F'_{\mathrm{upper}} = 1 - N \left(p_{01} + \sum_{i=1}^{3} p_{0i} \right). \tag{4.18}$$

We note for completeness that if the final two CNOT gates are set in the same direction (e.g., both the CNOT gates are controlled by the source qubit) one of the preceding $\sigma_i^{(\mathrm{s})}$ errors on the source qubit cannot be detected, commuting with both the final two gates, to lower the fidelity. These upper bounds F_{upper} and F'_{upper} coincide with each other for the uniform distribution of the gate errors $p_{ij} = p_g/15$ ($ij \neq 00$). In general, the upper bound is given by $\max[F_{\mathrm{upper}}, F'_{\mathrm{upper}}]$ depending on the error distribution; in a recurrence protocol one should determine whether the purification procedure is finished at an even or odd round. Other two-qubit Clifford gates instead of CNOT gates may also be used. Then, we obtain a similar upper bound with a suitable permutation among p_{ij}'s in Eq. (4.17) or Eq. (4.18) by counting the undetectable errors.

The recurrence protocols considered in Sec 4.2, with either single or double selection, have the setup as shown in Fig. 4.6 by the exchange of the directions of the CNOT gates in each round. In the single selection (Fig. 4.1), however, the σ_3 (σ_1) error on the ancilla $\rho^{(1)}$ cannot be detected by the Z (X) measurement, while the σ_1 and σ_2 (σ_2 and σ_3) errors are detected. The double selection (Fig. 4.2) is designed to detect even the σ_3 (σ_1) error on the primary ancilla $\rho^{(1)}$ [(a1) and (a2)] by using the secondary ancilla $\rho^{(2)}$ (not shown explicitly in Fig. 4.6). The errors on the source (s) are detectable if they leave any information on ancillae (a1) and (a2), that is, the ancilla errors play as the tracers of the source errors, as discussed so far. Thus in the double-selection protocol all the detectable errors on the source (s) are removed by detecting fully the errors on ancillae (a1) and (a2)

in the first order with the help of the extra ancillae. The upper bound on the fidelity is almost saturated as

$$F_{\max}^{\mathcal{D}} = F_{\text{upper}} - O(p_e^2) \tag{4.19}$$

up to the higher-order error contributions $\sim p_e^2 = p_g^2, p_g p_m, p_m^2$. This estimate has been confirmed by the numerical calculation for $p_g < 2\%$ almost independent of $p_m < 5\%$ in Sec. 4.2 (see Fig. 4.3).

On the other hand, in the single selection the would-be detectable error $\sigma_3^{(\text{s})} \otimes \sigma_1^{(\text{a2})}$ of the second-to-final CNOT gate in Fig. 4.6, in addition to the undetectable error $\sigma_3^{(\text{s})} \otimes \sigma_0^{(\text{a2})}$, is not detected by the X measurement of ancilla (a2). As a result, these two σ_3 errors are left on the source (s) after the second-to-final round of purification. This is just the same for ancilla (a1). The two σ_3 errors on the ancilla (a1) are not detected by the Z measurement of ancilla (a1), and they are propagated to the source (s) as the two σ_3 errors through the final CNOT gate. The would-be detectable errors $\sigma_i^{(\text{s})} \otimes \sigma_3^{(\text{a1})}$ of the final CNOT gate are not detected either by the Z measurement of ancilla (a1). Due to these would-be detectable errors, but are not detected in practice, the achievable fidelity of the single-selection protocol is lowered from that of the double-selection protocol as

$$F_{\max}^{\mathcal{S}} = F_{\max}^{\mathcal{D}} - N(6/15)p_g - O(p_e^2) \tag{4.20}$$

with $p_{ij} = p_g/15$ $(ij \neq 00)$. This estimate on $F_{\max}^{\mathcal{S}}$ in the low noise regime has also been confirmed by the numerical calculation in Sec. 4.2.

The above limitation on the achievable fidelity, which is due to the errors introduced by some gate operations in the final stage, is applicable to a wide variety of purification protocols. The purification protocols proposed so far [77, 86, 87, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124] do not achieve the fidelity higher than $F_{\max}^{\mathcal{S}}$ of the single selection. Specifically, in the protocol of Ref. [119] for large two-colorable graph states, which has an apparently similar setup to the double selection, the source state is connected with the two ancilla states by the two CNOT gates in order to extract sufficiently the error syndrome of the source state for the error correction. It is, however, realized that this setup just implements twice the error detections for the single selections. (The ancilla states are not inspected by using other ancilla states and CNOT gates. This is clearly different from the double selection.) Furthermore, one of the preceding errors on the source state cannot be detected, commuting with the two CNOT gates set in the same

direction, as discussed so far. As a result, the achievable fidelity of this protocol [119] becomes lower than that of the single-selection protocol [86, 87].

In the protocol of Ref. [124], $N-1$ EPR pairs are purified from noisy N EPR pairs by the single selection in order to improve the yield under perfect local operations for $N \geq 3$. An N to $N-2$ protocol with double selection may be considered as an extension to improve the achievable fidelity. However, the coincidence of all successful operations is required to pass the verification process with either single or double selection. Thus, as N increases the success probability for purification decreases substantially due to the multiple errors in the N to $N-1$ (or N to $N-2$) protocol. This indicates that the yield is not improved significantly in this sort of extension under imperfect local operations. We have made some numerical calculations for the 3–2 protocol with single selection and for the 4–2 protocol with double selection. The resultant yields $Y(F = 0.9, F_{\rm ch} = 0.8)$ with $p_g = p_m = 0.01$ are 0.025 and 0.085 for the 3–2 (single) and 4–2 (double) protocols, respectively, while $Y = 0.15$ and 0.085 for the usual 2–1 (single) and 3–1 (double) protocols, respectively. On the other hand with $p_g = p_m = 0.02$, the 3–2 (single) protocol cannot achieve $F = 0.9$, and $Y = 0.030$ for the 4–2 (double) protocol, while $Y = 0.060$ and 0.055 for the usual 2–1 (single) and 3–1 (double) protocols, respectively. These results support the argument that this sort of extension does not improve the yield under imperfect local operations. Optimization for yield might be possible by combining the double selection with some appropriate methods, although it is beyond our scope.

The triple (or more) selection by using three ancilla EPR pairs also removes fully the detectable first-order errors, achieving the same $F_{\rm upper}$ in the low noise regime as the double selection. It may further remove the higher-order errors to improve the fidelity and the noise threshold. We have considered a protocol with triple selection, which has a better noise threshold of 4.9% approaching the upper bound 5.3% [125], although it is not a purpose of the present study to pursue this possibility.

4.4 Multipartite entanglement purification

Recently purification is applied to a large class of multipartite entanglements including two-colorable graph states [86, 87, 119, 121, 123]. We can extend the present double-selection scheme for multipartite entanglement purification. Specifically, here we consider the purification of two-colorable graph states.

A graph is a set of vertices V connected in a specific way by edges E. Then a stabilizer operator K_j is defined associated with each vertex V_j as

$$K_j = X_j \bigotimes_{\{k,j\}\in E} Z_k, \tag{4.21}$$

where V_k are the neighboring vertices connected with V_j by edges, and the Pauli operators X_j and Z_k ($X \equiv \sigma_1$ and $Z \equiv \sigma_3$) act on the qubits on V_j and V_k, respectively. [126]. A graph state $|\mu_1\mu_2\cdots\mu_N\rangle$ is an eigenstate of this set of stabilizer operators as

$$K_j|\mu_1\mu_2\cdots\mu_N\rangle = (-1)^{\mu_j}|\mu_1\mu_2\cdots\mu_N\rangle(\mu_j = 0, 1). \tag{4.22}$$

Especially, here we consider graph states associated with a two-colorable graph where the vertices are divided into two sets (colors) A and B in such a way that no vertices within one set are connected by edges. Namely two-colorable graph states are described as

$$|\boldsymbol{\mu}_A, \boldsymbol{\mu}_B\rangle, \tag{4.23}$$

where $\boldsymbol{\mu}_A$ and $\boldsymbol{\mu}_B$ denote the sets of the eigenvalues of the stabilizers with colors A and B, respectively.

The entanglement purification with double selection for a noisy mixture of two-colorable graph states

$$\rho = \sum_{\boldsymbol{\mu}_A,\boldsymbol{\mu}_B} \lambda_{\boldsymbol{\mu}_A,\boldsymbol{\mu}_B}|\boldsymbol{\mu}_A, \boldsymbol{\mu}_B\rangle\langle\boldsymbol{\mu}_A, \boldsymbol{\mu}_B| \tag{4.24}$$

is implemented as follows (see Fig. 4.7):

(i) Alice, Bob, $\cdots$, Nancy share three identical two-colorable graph states $\rho^{(0)}$, $\rho^{(1)}$ and $\rho^{(2)}$ through a noisy quantum channel. This means that the qubits at each party have the same color, i.e., the party has its own color A or B.

(ii) They operate a multi-lateral CNOT gate on $\rho^{(0)}$ and $\rho^{(1)}$, where for color A $\rho^{(0)}$ and $\rho^{(1)}$ are taken as the control and the target, respectively, while for color B $\rho^{(0)}$ and $\rho^{(1)}$ are taken as the target and the control, respectively

(iii) Next they operate a multi-lateral CNOT gate on $\rho^{(2)}$ and $\rho^{(1)}$, similarly to the case of $\rho^{(0)}$ and $\rho^{(1)}$.

(iv) They make multi-lateral measurements, where for color A $\rho^{(1)}$ and $\rho^{(2)}$ are measured in the Z and X bases, respectively, while for color B $\rho^{(1)}$ and $\rho^{(2)}$ are measured in

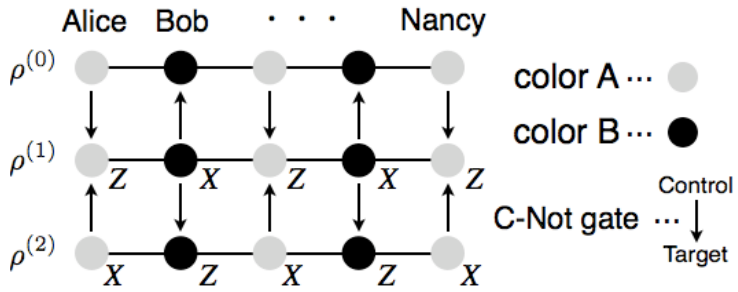


Figure 4.7: Purification of two-colorable graph states with double selection.

the X and Z bases, respectively. The party i with color A obtains the outcomes $(-1)^{\xi_i^{(1)}}$ and $(-1)^{\xi_i^{(2)}}$, while the party j with color B obtains the outcomes $(-1)^{\zeta_j^{(1)}}$ and $(-1)^{\zeta_j^{(2)}}$, where $\xi, \zeta = 0, 1$.

(v) They keep $\rho^{(0)}$ if for all of them (i and j) $\xi_i^{(2)} \oplus \sum_{\{k,i\}\in E} \zeta_k^{(2)} = 0$, and $\zeta_j^{(1)} \oplus \sum_{\{k,j\}\in E} \xi_k^{(1)} = 0$, which implies $\boldsymbol{\mu}_B^{(1)} \oplus \boldsymbol{\mu}_B^{(2)} = \mathbf{0}$, and $\boldsymbol{\mu}_A^{(0)} \oplus \boldsymbol{\mu}_A^{(1)} \oplus \boldsymbol{\mu}_A^{(2)} = \mathbf{0}$, respectively, where $\oplus$ denotes bitwise addition modulo 2.

They iterate procedures (ii)–(v) by using the output states which survive the selection in procedure (v) as the input states for the next round where the X and Z bases of their reference frames are exchanged with a Hadamard transformation. Note in Fig. 4.7 that the source state $\rho^{(0)}$ and the two ancilla states $\rho^{(1)}$ and $\rho^{(2)}$ are connected by the two multi-lateral CNOT gates in the same way as the bipartite case for the double selection to remove fully the detectable errors on $\rho^{(0)}$ in the first order. This setup is distinct from that of Ref. [119].

We apply this double-selection protocol specifically to the Steane seven-qubit code state (a CSS code state) as an example of two-colorable graph states, and compare it in performance with the Aschauer-Dür-Briegel (ADB) protocol of single selection [86, 87]. We consider a multi-party communication situation, where the N-qubit two-colorable graph states of $|\mathbf{0}_A, \mathbf{0}_B\rangle$ are shared through N identical noisy channels $\mathcal{C}^{\otimes N}$. Then the noisy copies of $\rho_{\rm in} = \mathcal{C}^{\otimes N}(|\mathbf{0}_A, \mathbf{0}_B\rangle\langle\mathbf{0}_A, \mathbf{0}_B|)$ are purified with the noisy CNOT gates and measurements. We have simulated directly the noisy operations on the code states in the communication channels and the purification procedures by using the Monte-Carlo method. (It is very complicated in the high dimensional space to provide the purification map in terms of the transition probability tensor.) The fidelity of the purified state ρ' is

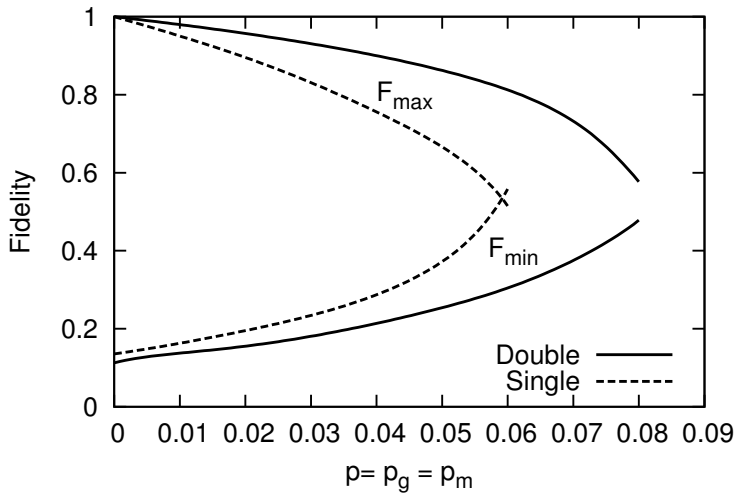


Figure 4.8: Maximum achievable fidelity $F_{\max}$ (upper curves) and minimum required initial fidelity $F_{\min}$ (lower curves) for the Steane seven-qubit code state $|0_L\rangle$ are plotted as functions of the error probability $p = p_g = p_m$ for the single and double selections.

measured by

$$F(\rho', |\mathbf{0}_A, \mathbf{0}_B\rangle) = \langle \mathbf{0}_A, \mathbf{0}_B | \rho' | \mathbf{0}_A, \mathbf{0}_B \rangle. \tag{4.25}$$

If the initial fidelity

$$F_{\rm in} \equiv F(\rho_{\rm in}, |\mathbf{0}_A, \mathbf{0}_B\rangle) = F_{\rm ch}^7 + O((1 - F_{\rm ch})^3) \tag{4.26}$$

is higher than $F_{\min}$, we can achieve the fidelity $F_{\max}$ by iterating the purification procedure.

The resultant maximum achievable fidelity $F_{\max}$ and the minimum required initial fidelity $F_{\min}$ are plotted in Fig. 4.8 for the Steane seven-qubit code state $|\mathbf{0}_A, \mathbf{0}_B\rangle = |0_L\rangle$ as functions of the error probability $p = p_g = p_m$, where $r_i = 1/3$ is taken typically for the error probabilities of the noisy communication channel $\mathcal{C}$ in Eq. (4.13). As expected, the double selection achieves the considerably higher fidelity $F_{\max}$ with lower minimum required initial fidelity $F_{\min}$ in comparison with the single selection [86, 87]. It really saturates the upper bound $F_{\max}^{\mathcal{D}} \approx F_{\rm upper} = 1 - 7(4/15)p_g$ for $N = 7$ with $p_{ij} = p_g/15$ $(ij \neq 0)$ of Eq. (4.17) in the low noise regime. The noise threshold for the local operations is also improved from 5.9% (single) to 8.2% (double) for $p = p_g = p_m$. It is also seen in Fig. 4.9 ($F_{\rm in} \simeq 0.48$ for $F_{\rm ch} = 0.9$ typically) that both schemes provide comparable yields, similar to the bipartite case. The yields are, however, significantly lower than those of the bipartite case. This is because the coincidence of the more measurement outcomes is required in the multipartite case so that the success probability of postselection is reduced.

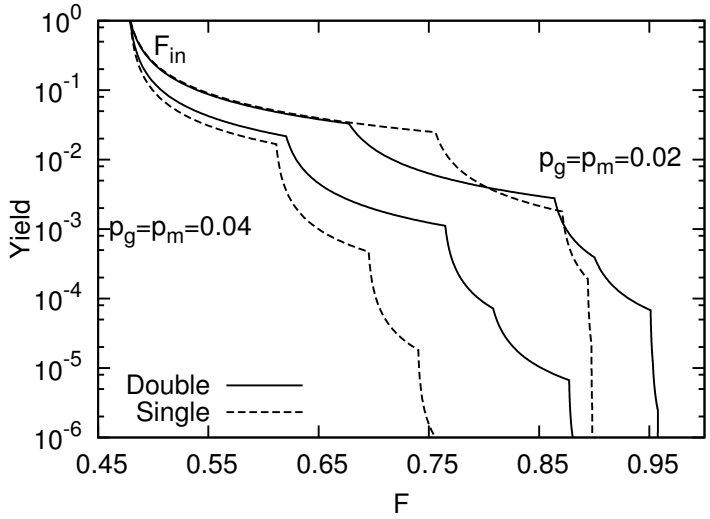


Figure 4.9: The yield $Y_{\mathcal{A}}(F, F_{\rm ch} = 0.9)$ is plotted as a function of the target fidelity F for each protocol with $p_g = p_m = 0.02$ (upper curves) and $p_g = p_m = 0.04$ (lower curves).

The two-colorable graph states, including CSS code states and cluster states, play important roles in quantum computation as well as quantum communication. Then these results really indicate that the double selection is profitable also in quantum computation. In fact, encoded ancilla qubits are used to stabilize a computation in a fault-tolerant way, and the performance of computation highly depends on the fidelity of these ancilla qubits [20, 27]. In the usual fault-tolerant context [20, 83, 89], these encoded ancilla qubits are prepared through the single selection. Thus the double selection has a good potential to improve the noise threshold of fault-tolerant computation. In Chapter 3, the verification process with double selection is used in fault-tolerant computation with concatenated construction of verified logical cluster states, where a considerably high noise threshold $\sim 3\%$ is achieved [29].

4.5 Conclusion

We have investigated entanglement purification with double selection under imperfect local operations. It has been shown that the double-selection protocol improves significantly the purification performance compared with the usual protocol with single selection. That is, the double-selection protocol has higher noise thresholds for the local operations and communication channels, and achieves higher fidelity of purified states. It also provides a reasonable yield comparable to or even better than that of the single selection. It has

been shown that the purification fidelity is limited by the intrinsically undetectable errors, which are introduced by the final gate operations. The double selection is a simple method to remove certainly all the detectable errors in the first order so that it achieves the upper bound on the fidelity in the low noise regime. The double selection has been further applied to the purification of multipartite entanglement, specifically two-colorable graph states. The improvement of the fidelity and noise threshold has been shown for the Steane seven-qubit code state as a typical example. The double selection can be extended for various graph states in the same way. These results really indicate that the double selection is profitable for entanglement-based protocols. Since multipartite entangled states, such as CSS codes and cluster states, play important roles in quantum computation as well as quantum communication, the double selection has a good potential to improve the performance of quantum computation.

Appendix B
Transition probability tensors

The transition probability tensors to characterize the purification maps are calculated by tracing the linear transformations of Bell states through the purification procedures. In the single-selection protocol the linear transformation $\tilde{\mathcal{S}}$ of two Bell states $\phi_i^{(0)} \otimes \phi_j^{(1)}$ before the postselection is given as

$$\tilde{\mathcal{S}}(\phi_i^{(0)} \otimes \phi_j^{(1)}) = \tilde{S}_{kl}^{ij} \phi_k^{(0)} \otimes \phi_l^{(1)}, \tag{4.27}$$

which provides $\tilde{\mathcal{S}}(\rho^{(0)} \otimes \rho^{(1)}) = F_i F_j \tilde{S}_{kl}^{ij} \phi_k^{(0)} \otimes \phi_l^{(1)}$. This map consists of the noisy bilateral CNOT gate $\mathcal{G}(\phi_i^{(0)} \otimes \phi_j^{(1)}) = G_{ab}^{ij} \phi_a^{(0)} \otimes \phi_b^{(1)}$, the error effect on the ancilla $\phi_b^{(1)}$ in the bilateral Z measurement $\mathcal{M}(\phi_b^{(1)}) = M_l^b \phi_l^{(1)}$, and the bilateral Hadamard operation $\mathcal{H}(\phi_a^{(0)}) = H_k^a \phi_k^{(0)}$ to describe mathematically (perfect by itself) the change in the reference frames for the next round,

$$\tilde{S}_{kl}^{ij} = H_k^a M_l^b G_{ab}^{ij}. \tag{4.28}$$

The noisy bilateral CNOT gate G_{km}^{ij} is decomposed into the ideal one U_{ab}^{ij} and the bilateral combination $N_{km}^{cd} N_{cd}^{ab}$ of the noises as follows:

$$G_{km}^{ij} = N_{km}^{cd} N_{cd}^{ab} U_{ab}^{ij}. \tag{4.29}$$

The ideal bilateral CNOT gate operation $\mathcal{U}^{\otimes 2} \equiv \mathcal{U}_A \otimes \mathcal{U}_B$ with the local operations at Alice (A) and Bob (B) induces the permutation U_{ab}^{ij} among $\phi_i^{(0)} \otimes \phi_j^{(1)}$'s. To find U_{ab}^{ij} we

use suitably the graph-state representation as

$$|\phi_i\rangle \equiv (I \otimes H)|\mu_A^i, \mu_B^i\rangle, \tag{4.30}$$

where

$$\boldsymbol{\mu}^i = (\mu_A^i, \mu_B^i) = (0,0), (1,0), (1,1), (0,1) \tag{4.31}$$

for $i = 0, 1, 2, 3$, respectively. The action of bilateral CNOT gate on the graph states, $|\mu_A^i, \mu_B^i\rangle^{(0)}|\mu_A^j, \mu_B^j\rangle^{(1)} \to |\mu_A^i, \mu_B^i \oplus \mu_B^j\rangle^{(0)}|\mu_A^i \oplus \mu_A^j, \mu_B^j\rangle^{(1)}$, is denoted simply as

$$\tilde{\mathcal{U}}(\boldsymbol{\mu}^i \otimes \boldsymbol{\mu}^j) = (\mu_A^i, \mu_B^i \oplus \mu_B^j) \otimes (\mu_A^i \oplus \mu_A^j, \mu_B^j). \tag{4.32}$$

Then the permutation is read as

$$U_{ab}^{ij} = \begin{cases} 1 & [\boldsymbol{\mu}^i \otimes \boldsymbol{\mu}^j = \tilde{\mathcal{U}}(\boldsymbol{\mu}^a \otimes \boldsymbol{\mu}^b)] \\ 0 & [\boldsymbol{\mu}^i \otimes \boldsymbol{\mu}^j \neq \tilde{\mathcal{U}}(\boldsymbol{\mu}^a \otimes \boldsymbol{\mu}^b)] \end{cases} . \tag{4.33}$$

For example, $U_{22}^{13} = 1$ for $\tilde{\mathcal{U}}[\boldsymbol{\mu}^2 \otimes \boldsymbol{\mu}^2 = (1,1) \otimes (1,1)] = \boldsymbol{\mu}^1 \otimes \boldsymbol{\mu}^3 = (1,0) \otimes (0,1)$, and $U_{ij}^{13} = 0$ for the others, providing $\mathcal{U}^{\otimes 2}(\phi_1^{(0)} \otimes \phi_3^{(1)}) = U_{ij}^{13}\phi_i^{(0)} \otimes \phi_j^{(1)} = \phi_2^{(0)} \otimes \phi_2^{(1)}$. The noise map of the CNOT gate at one party in Eq. (4.4) is specified for the basis states $\phi_a^{(0)} \otimes \phi_b^{(1)}$ as

$$\begin{aligned} \mathcal{N}(\phi_a^{(0)} \otimes \phi_b^{(1)}) &= \sum_{ij} p_{ij}(\sigma_i \phi_a^{(0)} \sigma_i) \otimes (\sigma_j \phi_b^{(1)} \sigma_j) \\ &= N_{cd}^{ab} \phi_c^{(0)} \otimes \phi_d^{(1)}, \end{aligned} \tag{4.34}$$

where σ_i and σ_j act on the control and target qubits at the party, respectively. This formula is applied equally to the CNOT gate operations by Alice and Bob. The operations by σ_i and σ_j in Eq. (4.34) induce the permutations among the Bell states as $\mathcal{P}_{\sigma_i}(\phi_a) = \sigma_i \phi_a \sigma_i = \phi_c$, which are given explicitly by

$$\begin{aligned} \mathcal{P}_{\sigma_0} &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}, \mathcal{P}_{\sigma_1} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}, \\ \mathcal{P}_{\sigma_2} &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}, \mathcal{P}_{\sigma_3} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix}, \end{aligned} \tag{4.35}$$

e.g., $\sigma_1 \phi_2 \sigma_1 = \phi_3$ is given as $2 \to 3$ in $\mathcal{P}_{\sigma_1}$, and so on. This reads

$$N_{cd}^{ab} = p_{ij}[(ac) \in \mathcal{P}_{\sigma_i}, (bd) \in \mathcal{P}_{\sigma_j}], \tag{4.36}$$

e.g., $N_{10}^{00} = p_{10}$ for $(ac) = (01)$ and $(bd) = (00)$, and so on. Then the bilateral combination of the deporalizing errors is given by

$$\mathcal{N}_B[\mathcal{N}_A(\phi_a^{(0)} \otimes \phi_b^{(1)})] = N_{km}^{cd} N_{cd}^{ab} \phi_k^{(0)} \otimes \phi_m^{(1)}, \tag{4.37}$$

where $\mathcal{N}_A$ and $\mathcal{N}_B$ represent the noise maps of Eq. (4.34) at Alice and Bob, respectively.

The imperfect Z measurement by each party can be described equivalently as a sequence of a noise map

$$\mathcal{M}_e(\rho) = (1-p_m)\sigma_0\rho\sigma_0 + p_m\sigma_1\rho\sigma_1 \tag{4.38}$$

and the ideal measurement with the projection operators $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$. This is because the action of the POVM operators E_k in Eqs. (4.5) and (4.6) is reproduced by $|k\rangle\langle k|\mathcal{M}_e$ as $\mathrm{Tr}(E_k\rho) = \mathrm{Tr}[\mathcal{M}_e(|k\rangle\langle k|)\rho] = \mathrm{Tr}[|k\rangle\langle k|\mathcal{M}_e(\rho)]$ $(k = 0, 1)$ [114, 115]. Then the noise effect in the bilateral Z measurement is given by

$$M_l^b = m_l^f m_f^b \tag{4.39}$$

as a product of the single ones $\mathcal{M}_e(\phi_b) = m_f^b\phi_f$ in Eq. (4.38) with

$$m_f^b = \begin{cases} 1-p_m & [(bf) \in \mathcal{P}_{\sigma_0}] \\ p_m & [(bf) \in \mathcal{P}_{\sigma_1}] \\ 0 & [(bf) \in \mathcal{P}_{\sigma_2}, \mathcal{P}_{\sigma_3}] \end{cases} . \tag{4.40}$$

The bilateral Hadamard operation is given by

$$H_k^a = h_k^e h_e^a, \tag{4.41}$$

where the single operation $H|\phi_a\rangle = h_e^a|\phi_e\rangle$ is given with $h_0^0 = h_3^1 = h_2^2 = h_1^3 = 1$ and $h_e^a = 0$ for the others. This operation provides mathematically the inversion of the direction (control and target) of the CNOT gate in the next round, and the permutation of the error parameters is induced accordingly as

$$p_{ij} \to p'_{i'j'}[\sigma_{i'} = H\sigma_j H, \sigma_{j'} = H\sigma_i H], \tag{4.42}$$

that is, the components are exchanged as $i \leftrightarrow j$ and then $1 \leftrightarrow 3$ round by round. The uniform error distribution is specifically invariant as $p_{ij} = p'_{i'j'} = p_g/15$ $(ij \neq 00)$.

After all the transition probability tensor S_i^{jk} of the single selection is obtained by picking up the right states $\phi_0^{(1)}$ and $\phi_3^{(1)}$ $(l = 0, 3)$ from $\tilde{\mathcal{S}}(\rho^{(0)} \otimes \rho^{(1)}) = F_j F_k \tilde{S}_{il}^{jk} \phi_i^{(0)} \otimes \phi_l^{(1)}$, which pass the postselection after the Z measurement,

$$S_i^{jk} = \tilde{S}_{i0}^{jk} + \tilde{S}_{i3}^{jk}, \tag{4.43}$$

where the error parameters p_{ij} and p_m are included as seen so far. By taking the uniform error distribution $p_{ij} = p_g/15$ $(ij \neq 00)$ and then setting $p_g = p_m = 0$, this formula of S_i^{jk}

for the single selection really reproduces the purification maps presented in the preceding studies with imperfect [114, 115] and perfect [77, 116, 117] local operations, respectively.

Similarly, the purification procedure of the double selection before the postselection is described as a linear map $\tilde{\mathcal{D}}$ of $\phi_i^{(0)} \otimes \phi_j^{(1)} \otimes \phi_k^{(2)}$ as

$$\tilde{D}_{lmn}^{ijk} = H_l^a M_m^c \tilde{M}_n^d G_{dc}^{kb} G_{ab}^{ij}, \tag{4.44}$$

where

$$\tilde{M}_n^d = H_n^f M_f^e H_e^d \tag{4.45}$$

provides the noise effect in the bilateral X measurement. Then the transition probability tensor of the double selection is obtained by the postselection after the Z and X measurements as

$$D_i^{jkl} = \sum_{m=0,3;n=0,1} \tilde{D}_{imn}^{jkl}. \tag{4.46}$$

Chapter 5

Topological one-way quantum computation on verified logical cluster states

In this chapter, we present a scheme to improve the noise threshold for the fault-tolerant topological one-way computation with a constant overhead. Certain cluster states of finite size, say star clusters, are constructed with logical qubits through an efficient verification process to achieve high fidelity. Then, the star clusters are connected near-deterministically with verification to form a three-dimensional cluster state to implement the topological one-way computation. The necessary postselection for verification is localized within the star clusters, ensuring the salability of computation. By using the Steane seven-qubit code for the logical qubits, this scheme works with a high error rate 2% and reasonable resources comparable to or less than those for the other fault-tolerant schemes. A higher noise threshold would be achieved by adopting a larger code.

5.1 Introduction

The issue of decoherence is one of the most important obstacles for realization of quantum information processing. To overcome this problem, fault-tolerant computation based on quantum error correction (QEC) codes has been developed [10, 11, 12, 36, 79, 80]. The main achievement of the quantum fault-tolerant theory is the threshold theorem; if the amount of noise per gate is smaller than a certain value, namely the noise threshold, quantum computation can be performed to arbitrary accuracy with a polynomial overhead [13, 14, 15, 16, 17]. The noise threshold have been calculated to be about $10^{-4} - 10^{-2}$ for a variety of fault-tolerant schemes based on concatenated QEC codes [19, 20, 21, 23, 24, 25].

Besides this standard QEC method, there is a different promising approach for fault-tolerance, where a surface code protects information by virtue of topological degeneracy, without requiring concatenation [90, 91]. Then, one-way computation (OWC) [41, 42] with the topological fault-tolerance can be performed on a three-dimensional (3D) cluster state [92, 94]. Furthermore, the 3D system is mapped to a two-dimensional (2D) lattice [93, 94]. The topological computation can be performed only with nearest-neighbor two-qubit gates. These 2D and 3D computations achieve noise thresholds 0.75% and 0.67%, respectively.

On the other hand, if one needs to perform computation by using noisy devices with an error rate $\sim 1\%$, some different approaches or additional ingredients will be required. We here consider to integrate the QEC encoding and postselection into the topological one-way computation (TOWC) in a 3D cluster state. In an early approach, improved preparation of encoded ancilla states with postselection is considered [20, 107]. Then, such an approach is applied to the OWC with off-line preparation of logical qubits and cluster states [28, 105, 106]. The postselection to reduce the logical error efficiently, however, appears to have trouble with scalable computation. This dilemma between postselection and scalability has been solved recently in a cluster-based architecture by using the unique feature of OWC [25].

In this chapter, we present an efficient method to construct arbitrary large cluster states of logical qubits with high fidelity, where postselection is adopted for verification being reconciled with scalability. Then, we apply this method to the TOWC in 3D cluster states to improve its noise threshold. That is, the TOWC is performed by using logical qubits, where the logical degree of freedom is utilized to reduce the logical measurement errors. This is viewed as concatenation of the topological surface code with a suitable QEC code. The whole procedure consists of (i) *logical cluster-state preparation with verification*, (ii) *near-deterministic connection with verification*, and (iii) *TOWC by measuring the logical qubits*. At the stage (i) a specific finite-size cluster state of logical qubits is copiously prepared off-line with postselection through an efficient verification process based on syndrome extraction [25]. At the stage (ii) these cluster states are connected near-deterministically with verification to form scalably a 3D cluster state of logical qubits. This verification process removes the additional errors introduced by the gate operation for the connection, keeping clean enough the logical qubits in the 3D cluster state to implement the TOWC below the threshold of the surface code at the stage (iii). Since the

encoding and verification processes require nonlocal two-qubit gates at the physical level, the present scheme loses the good geometrical property of the topological computations. It will be nevertheless worth realizing quantum computation with a high error rate $\sim 1\%$ and a reasonable overhead.

The rest of this chapter is organized as follows. In Sec. 5.2, we describe how to construct a specific type of cluster state, say *star cluster*, with logical qubits. The star cluster of logical qubits is constructed with high fidelity through verification process, namely *double verification*. In Sec. 5.3 the star clusters are connected near-deterministically to form a 3D cluster state of logical qubits for topological one-way computation. The performance of this scheme is analyzed in Secs. 5.4 and 5.5, with respect to the noise threshold and resources usage, respectively. Then, some possible improvements of performance are considered in Sec. 5.6. Section 5.7 is devoted to summary and conclusion.

5.2 Star clusters through double verification

We can reduce the effective measurement error in OWC by replacing each physical qubit with a logical one [25, 28, 105, 106]. It is, however, not a trivial task to prepare such large entangled states as cluster states of logical qubits with high fidelity. To this end a finite-size cluster state of logical qubits, say *"star cluster"*, is prepared via verification, which consists of one *"root node"* located at the center and surrounding L *"leaf nodes"*, as shown in Fig. 5.1 (a).

Starting with physical qubits, QEC code states $|0_L\rangle$ and $|+_L\rangle = (|0_L\rangle + |1_L\rangle)/\sqrt{2}$ are first encoded by means of noisy gate operations as usual. We adopt specifically the Steane seven-qubit code, which is the minimum self-dual CSS (Calderbank-Shor-Steane) code with distance three [79, 80]. The logical qubits are verified by detecting elaborately the error syndrome with primary and secondary ancilla qubits attached through transversal controlled-NOT (CNOT) and controlled-Z (CZ) gates, namely the double verification, as shown in diagram (3.17) in Chapter 3. This double verification can detect optimally the first-order errors, as discussed in Chapters 3 and 4 [25, 30]. The verified logical qubits are next connected with transversal CZ gates to form cluster states of two logical qubits. The errors left on each qubit through the CZ gate operations are inspected further by the double verification. Finally, L verified two-qubit cluster states and a single logical qubit are combined via transversal CZ gates with the double verification to form a star cluster

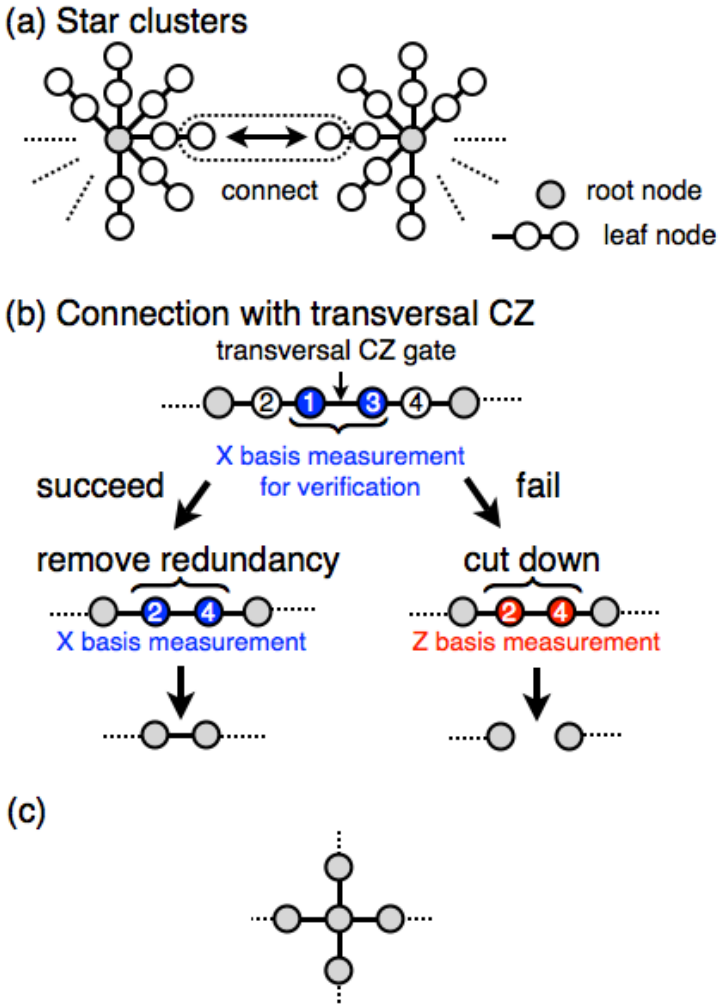


Figure 5.1: (a) Star clusters to be connected. (b) Verification of the transversal CZ gate by measuring the qubits 1 and 3. If the connection succeeds, the redundant qubits 2 and 4 are removed (left). Otherwise, the connection is abandoned (right). (c) By repeating this process, the root nodes are connected to form a cluster state.

with L leaf nodes, as shown in Fig. 5.1 (a).

Since all the verification procedures are transversal, it is reasonably expected that the error distribution on each qubit in a resultant star cluster is independent and identical, namely *homogeneous* [27]. The errors on each qubit ρ at the physical level are well approximated by

$$(1-p)\rho + \sum_{A=X,Y,Z} \epsilon_A A\rho A \tag{5.1}$$

with probabilities $\epsilon_A = r_A p$, which are determined in terms of the noise parameters characterized by a mean error rate p. Here, we adopt the usual noise model: (i) A two-qubit gate is followed by $A\otimes B$ errors with probabilities p_{AB} ($A, B = I, X, Y, Z$, and $AB \neq II$). (ii) The preparation and measurement of physical qubits are implemented with error probabilities p_P and p_M, respectively. In particular, $(p_{AB}, p_P, p_M) = (p/15, 4p/15, 4p/15)$ is employed in the following analysis [20, 25]. As discussed in Chapters 3 and 4, the double verification optimaly reduce the first order errors. The homogeneous error probabilities ϵ_A of the output state are calculated in the leading order in Eq. (3.31). They are given for $p_{AB} = p/15$ as

$$(\epsilon_X, \epsilon_Y, \epsilon_Z) = (p/15, p/15, 2p/15), \tag{5.2}$$

which is in a good agreement with the numerical result for $p \leq 2\%$ in Fig. 3.1 of Chapter 3 [25, 30]. The homogeneity of the output errors has been further checked numerically for $p \leq 5\%$; the probability of correlated errors are are at least one order of magnitude smaller than that of two simultaneous independent errors.

Given the homogeneous errors in Eq. (5.1), the error probability for the X-basis measurement of a single logical qubit in the star cluster is calculated as

$$p_q^{(1)} \simeq f(p_q^{(0)}) \tag{5.3}$$

with the error probability $p_q^{(0)}$ in measuring each physical-level qubit as

$$p_q^{(0)} = \epsilon_Z + \epsilon_Y + p_M, \tag{5.4}$$

which is $(7/15)p$ in the leading order with the double verification. Specifically for the seven-qubit code, $p_q^{(1)} = 21(p_q^{(0)})^2 + \ldots$ with $f(x) = 1-(1-x)^7 - 7x(1-x)^6$. The logical measurements in the Z and Y bases are less noisy than that in the X basis with $\epsilon_Z > \epsilon_Y, \epsilon_X$ for the double verification; otherwise the modification of $p_q^{(0)}$ is straightforward.

5.3 Scalable construction of a 3D cluster state

We can construct a cluster state of an arbitrary size scalably by connecting the leaf nodes of the star clusters with the transversal CZ gates, as illustrated in Fig. 5.1. Since additional errors are introduced by the CZ gate operations, they should be removed by a suitable verification, which introduces nondeterminism of postselection to the connection process. The situation is somewhat similar to the linear optical quantum computation, where two-qubit gates are intrinsically nondeterministic [49, 50, 51, 61, 62]. Thus, we follow the so-called *divide and conquer* approach [49, 61, 62], except that even if the connection has failed after all, the cluster states are still connected erroneously (in the case of the linear optical fusion gate, the failure event results in a disconnected cluster state).

Specifically, in order to connect two neighboring root nodes, the CZ gates are operated between the ends of the two leaf nodes, as shown in Fig. 5.1 (b). Then, the connected qubits are measured in the logical X basis for verification. If no errors are detected, the redundant qubits are removed by measuring them in the X-basis, and the two root qubits are connected reliably. On the other hand, if infection of error is found, the noisy connection is abandoned by measuring the redundant qubits in the Z basis. The success probability of this connection is estimated for the seven-qubit code as

$$p_{\rm s} \simeq (1-p_G)^7(1-\epsilon_X-\epsilon_Y-\epsilon_Z)^{14}(1-p_M)^{14}. \tag{5.5}$$

Here, $p_G = 4p/5$ for the errors of the CZ gate except for $I\otimes X$, $X\otimes I$ and $X\otimes X$ commuting with the X-basis measurement. The error probability conditioned on the successful case $p_{\rm e/s}$ is quite small, since such events need simultaneous three errors for the seven-qubit code with distance three. It is calculated as

$$\begin{aligned} p_{\rm e/s} &= [2h(\epsilon_X+\epsilon_Z+p_{ZI}+p_{YI}+p_{ZX}+p_{ZY}+p_M) \\ &\quad +h(2\epsilon_Y+p_{ZZ}+p_{YY}+p_{ZY}+p_{YZ})]/p_s, \end{aligned} \tag{5.6}$$

where

$$h(x) = 1-\sum_{k=0}^{k=1}\left(\begin{array}{c}7\\k\end{array}\right) - 28x^3(1-x)^4 = 7x^3(1-x)^4+O(x^4). \tag{5.7}$$

Specifically for $p=1\%$, the conditional error probability is estimated to be $p_{\rm e/s}\sim 10^{-5}$, which is negligibly smaller than $p_q^{(1)}$. By making several attempts, we can surely connect

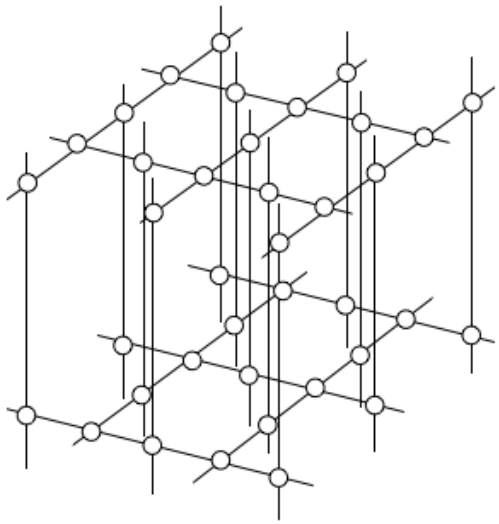


Figure 5.2: A 3D cluster state for TOWC, where each qubit is connected with four neighboring qubits in a specific way [92, 94]. In the present scheme, this cluster state is constructed by using the process in Fig. 5.1 so that each qubit is replaced by logical one with high fidelity.

the root nodes, as shown in Fig. 5.1 (c). If some or all of the connections have failed unfortunately after consuming the L leaf nodes, the erroneous connections are used as though they have succeeded. Such rare events can be included as the errors of logical qubits with a probability $p_{\rm fail}$, which will be calculated later.

In this way, we can connect scalably the root nodes to form an arbitrary cluster state of logical qubits for fault-tolerant one-way computation. Especially, the TOWC with a certain 3D cluster state is promising to improve significantly the noise threshold since the TOWC itself has a high noise threshold with the surface code [92, 93, 94]. A 3D cluster for TOWC is shown in Fig. 5.2, where each qubit is connected with four neighboring qubits in a specific way [92, 94]. In the present scheme, this cluster state is constructed by using the process in Fig. 5.1 so that each qubit is replaced by logical one with high fidelity.

5.4 Noise Threshold

If the error probability q for measuring a single logical qubit in the 3D cluster state is smaller than the threshold value of the surface code, the TOWC is performed fault-tolerantly. The noise threshold of the surface code with noisy syndrome measurements has been obtained to be 2.9 – 3.3 % from the random plaquetta Z(2) gauge theory [127, 128].

Thus, the threshold condition for the present scheme is given by

$$q = p_q^{(1)} + L p_q^{(1)} + p_{\rm fail} < 3.3\%. \tag{5.8}$$

The first and third terms, $p_q^{(1)}$ and $p_{\rm fail}$, are responsible for the logical measurement errors of the root qubit and the unsuccessful connection, respectively. The second term $Lp_q^{(1)}$ comes from the Pauli by-products which are introduced in removing the redundant qubits of the L leaf nodes by the X-basis (success case) or Z-basis (failure case) measurement. The number of leaf nodes L (> 4) is chosen to be sufficiently large, so that the failure probability of the connection is reduced as

$$p_{\rm fail} = \sum_{k=0}^{3} \left(\begin{array}{c} L \\ k \end{array} \right) p_{\rm s}^k (1-p_{\rm s})^{L-k} \sim \left(\begin{array}{c} L \\ 3 \end{array} \right) \times O(p^{L-3}) \tag{5.9}$$

with $1 - p_{\rm s} \sim O(p)$, where k represents the number of successful connections. Here, it should be noted that the error probability of the X-basis measurement conditioned on the correct syndrome for the verification, as shown in the first procedure of Fig. 5.1 (b), is estimated to be of higher order as $O(p^3)$ with the seven-qubit code, as calculated in Eq. (5.6). This error thus provides a negligible contribution in Eq. (5.8) compared with $p_q^{(1)} \sim O(p^2)$. Numerically, for example, for the mean error rate $p = 1\%$ (2%), the success probability is $p_{\rm s} \simeq 0.88$ (0.76) with the seven-qubit code. The number of leaf nodes is chosen to be $L = 7$ (9) so as to suppress the failure of connection as $p_{\rm fail} \sim 0.1\%$. Then, the error probability for the logical qubit becomes $q = 0.98\%(2.6\%)$ for $p = 1\%(2\%)$ in Eq. (5.8), which is smaller than the threshold value for the surface code. Universality can be obtained by using a noisy non-Clifford ancilla qubit and the magic state distillation [82]. The noise threshold for the magic state distillation has been calculated to be at least 6.3% [94]. Therefore, we can conclude that the noise threshold is 2% in the present scheme for the fault-tolerant universal TOWC.

5.5 Resources usage

The resources to implement a single two-qubit gate in the TOWC with logical qubits is calculated as $CR(q, \Omega)$ in terms of the resources for the TOWC $R(q, \Omega) = [\ln(10\Omega)/\kappa(q)]^3$ with $\kappa(q) \simeq (\ln 4q)/2$ [92], where q and Ω indicate the error probability and computation size, respectively. The constant overhead C for the logical encoding and verification is

given by

$$C \sim N(1-p)^{-K} \simeq Ne^{pK}, \tag{5.10}$$

where N is the number of physical qubits and gates per star cluster, and K is that of the error locations in the verification procedures, respectively. Strictly speaking, since simultaneous multiple errors may pass through the verification, the real constant overhead will be slightly smaller than Eq. (5.10). The resources for the verified star cluster N is given in terms of those N_1 and N_2 for the single and two-qubit logical cluster states, respectively:

$$N = \underbrace{(N_1 + LN_2 + 7L)}_{\text{star cluster}} + \underbrace{2(L+1)}_{\text{num. of ver.}}\Big(\underbrace{2N_1}_{\text{logical ancillae}} + \underbrace{14 \times 2}_{\text{gates in ver.}} \Big) = 2.9 \times 10^3 L + 1.0 \times 10^3, \tag{5.11}$$

where

$$N_1 = 3\Big[\underbrace{(9+7)}_{\text{qubits and gates in encoding}} \times 3 + \underbrace{14}_{\text{gates for the 1st ver.}} \Big] + \underbrace{14}_{\text{gates for the 2nd ver.}} \simeq 2 \times 10^2, \tag{5.12}$$

$$N_2 = \underbrace{(2N_1 + 7)}_{\text{2-qubit clus.}} + 2\Big(\underbrace{4N_1}_{\text{ancillae}} + \underbrace{14 \times 2}_{\text{gates in ver.}} \Big) \simeq 2 \times 10^3. \tag{5.13}$$

The error locations K are decomposed into the contributions K_1, K_2 and K_{star} from the single, two-qubit, and star cluster states, respectively:

$$pK = pK_1 + pK_2 + pK_{\text{star}} = (50L + 211)p, \tag{5.14}$$

where

$$\begin{aligned} pK_1 &= \underbrace{(9p + 7p_P)}_{\text{encoding}} \times 3 + \underbrace{2\left(9 \times 3\frac{p}{15} + 3p_P\right)}_{\text{ancillae}} + 2\Big(\underbrace{14p}_{\text{gates}} + \underbrace{14 \times p_M}_{\text{meas.}}\Big) \\ &\quad - \underbrace{(\epsilon_X + \epsilon_Y + \epsilon_Z) \times 7}_{\text{output}} \\ &\simeq 75p, \end{aligned} \tag{5.15}$$

$$\begin{aligned} pK_2 &= \underbrace{7p}_{\text{gates for 2-qubit clus.}} + 2\Big[\underbrace{7 \times 4(\epsilon_X + \epsilon_Y + \epsilon_Z)}_{\text{ancillae}} + \underbrace{14 \times 2p}_{\text{gates for ver.}} + \underbrace{14 \times 2p_M}_{\text{meas.}}\Big] \\ &\simeq 93p, \end{aligned} \tag{5.16}$$

$$\begin{aligned} pK_{\text{star}} &= \underbrace{7L}_{\text{gates for star clus.}} + \underbrace{2(L+1)}_{\text{num. of ver.}}\Big[\underbrace{7 \times 2(\epsilon_X + \epsilon_Y + \epsilon_Z)}_{\text{ancillae}} + \underbrace{14}_{\text{gates in ver.}} + \underbrace{14p_M}_{\text{meas.}}\Big] \\ &\simeq (50L + 43)p. \end{aligned} \tag{5.17}$$

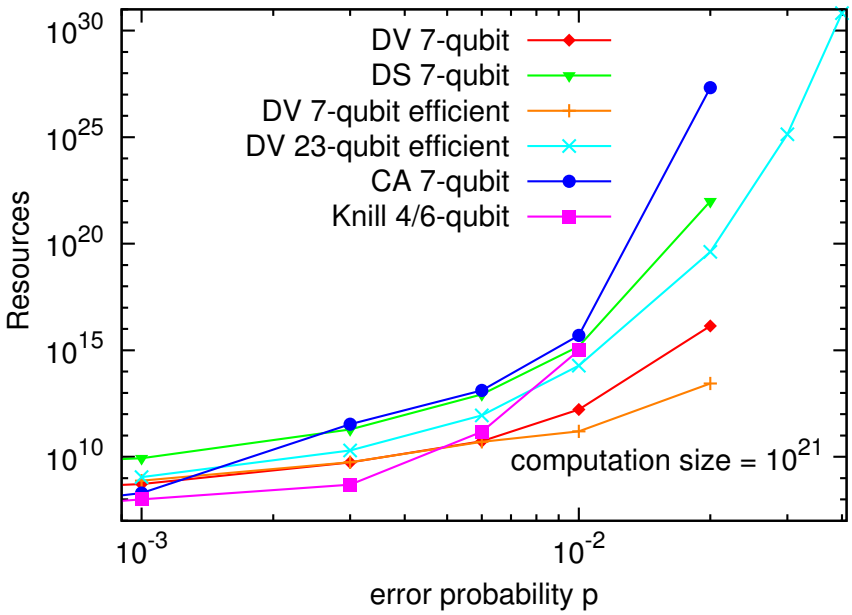


Figure 5.3: The resources per two-qubit gate for a computation size 10^{21} (gate accuracy $\sim 10^{-22}$) are plotted as functions of the error rate p for the present scheme with double verification (red $\Diamond$), the purification with double selection (blue $\triangledown$), the present scheme with an efficient star cluster construction (orange $+$), the present scheme with 23-qubit code (light blue $\times$), the cluster-based architecture (green $\bigcirc$) [25], and the Knill's error-correcting architecture (purple $\square$) [20].

The resources per two-qubit gate are plotted as functions of p in Fig. 5.3 for the present scheme with double verification (DV 7-qubit, red $\Diamond$) and the other competitive ones, the purification with double selection (DS 7-qubit, blue $\triangledown$) [30], the cluster-based architecture (CA 7-qubit, green $\bigcirc$) [25], and the Knill's error-correcting architecture (Knill 4/6-qubit, purple $\square$) [20]. For example, in the present scheme (DV 7-qubit), we estimate for $p = 1\%$ and $L = 7$ as $N \simeq 2 \times 10^4$, $K \simeq 6 \times 10^2$ and $C \sim 6 \times 10^6$. The overhead for the topological computation with $p = 1\%$ is given by $R(q = 0.98\%, \Omega = 10^{21}) \sim 3 \times 10^5$. Thus, the total overhead amounts to $CR \sim 2 \times 10^{12}$, which is less than those for the other schemes operated with an error rate $p = 1\%$. Some improvements of performance are possible as indicated with orange $+$ and light blue $\times$, which will be considered in the next section.

We may use the purification with double selection [30], instead of the double verification, for the star-cluster preparation (DS 7-qubit in Fig. 5.3), which also has the optimal performance for error detection with $(\epsilon_X, \epsilon_Y, \epsilon_Z) = (p/15, p/15, 2p/15)$ in the leading order. It, however, results in a lower success probability and a larger overhead than the double verification, since the coincidence of successful operations is required all over the

star cluster to pass the postselection. On the other hand, the double verification checks locally the erroneous sites which are connected by the CZ gates. This reduces the amount of successful coincidence, saving considerably the overhead for $p \sim 1\%$.

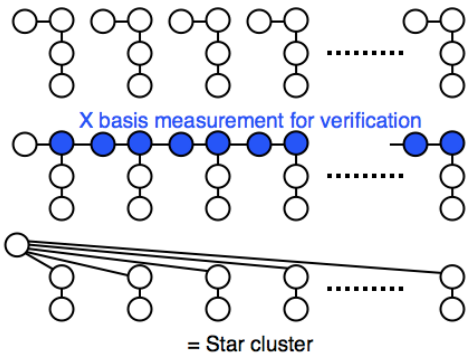
Although the cluster-based architecture suffers from memory errors in the concatenation of QEC code (CA 7-qubit in Fig. 5.3) [25], the present scheme without several concatenations does not accumulate the memory errors. The memory errors are simply added as $p_q^{(0)} + \tau p \simeq [(7/15) + \tau]p$, where τ denotes the effective waiting time. The waiting time τ required for the memory is rather limited, since we can run the TOWC on buffer nodes of finite size with constructing the 3D cluster states in parallel.

5.6 Improvement of the performance

We consider some possible improvements for the performance of the present scheme.

5.6.1 Efficient construction of the star cluster

We may start with preparing linear four-qubit logical cluster states through the double verification, rather than two-qubit ones. Then, the star clusters are constructed efficiently by connecting the four-qubit clusters with X-basis measurements for verification [53]:



(5.18)

In this case, the resources for the star cluster are given by

$$C \sim N_4 e^{pK_4} \times L \times p_s^{\log_2 L}. \tag{5.19}$$

The factor $N_4 e^{pK_4}$ indicates the resources for four-qubit linear cluster state, where N_4 and pK_4 are given by

$$N_4 = \underbrace{(2N_2 + 7)}_{\text{4-qubit clus.}} + 2\Big(\underbrace{4N_1}_{\text{ancillae}} + \underbrace{14 \times 2}_{\text{gates for ver.}} \Big) = 5.8 \times 10^3, \tag{5.20}$$

$$pK_4 = K_1 + 2K_2 \simeq 261p. \tag{5.21}$$

Compared with Eq. (5.10), the constant overhead for the star cluster construction is significantly reduced by virtue of parallelism, especially for an error rate $p \sim 2\%$ or higher. In Fig. 5.3, the resources for the efficient construction with the seven-qubit code is plotted as a function of the physical error probability p (orange +).

5.6.2 Large QEC code for a high noise threshold

A larger QEC code such as the concatenated seven-qubit code or the 23-qubit Golay code can be used to boost the noise threshold, since the double verification works even for $p = 5\%$ or higher, as indicated by a numerical simulation for the seven-qubit code. The distance of the 23-qubit Golay code is seven, and hence three errors can be corrected. The success probability of the verification is given naively by replacing 7 with 23 in Eq. (5.5) as

$$p_{\rm s} \simeq (1-p_G)^{23}(1-\epsilon_X-\epsilon_Y-\epsilon_Z)^{46}(1-p_M)^{46}. \tag{5.22}$$

Since this $p_{\rm s}$ is quite small, L becomes huge for the near-deterministic connection. We can avoid this trouble by correcting single qubit errors, which are most likely to occur. When the syndromes indicate two or more errors, the connection is discarded as usual. By using this adaptive strategy, the success probability is improved as

$$\begin{aligned} p_s &= (1-p_G)^{23}(1-\epsilon_X-\epsilon_Y-\epsilon_Z)^{46}(1-p_M)^{46} \\ &\quad +23p_G(1-p_G)^{22}(1-\epsilon_X-\epsilon_Y-\epsilon_Z)^{46}(1-p_M)^{46} \\ &\quad +46(\epsilon_X+\epsilon_Y+\epsilon_Z)(1-p_G)^{23}(1-\epsilon_X-\epsilon_Y-\epsilon_Z)^{45}(1-p_M)^{46} \\ &\quad +46p_M(1-p_G)^{23}(1-\epsilon_X-\epsilon_Y-\epsilon_Z)^{46}(1-p_M)^{45}. \end{aligned} \tag{5.23}$$

Specifically for $p = 3\%$ (4%), the success probability is calculated to be 0.63 (0.49). The conditional error probability $p_{\rm e/s}$ is obtained in Eq (5.6) by using

$$\begin{aligned} h(x) &= 1-\sum_{k=0}^{k=5}\left(\begin{array}{c}23\\k\end{array}\right)x^k(1-x)^{23-k} - 23\times 11\times 7\times 56x^6(1-x)^{17} \\ &= 23\times 11\times 7x^6(1-x)^{17} + 23\times 11\times x^7(1-x)^{16} + O(x^8). \end{aligned} \tag{5.24}$$

By virtue of the long distance, the conditional error probability is still sufficiently small $p_{\rm e/s} < 10^{-5}$ for $p \sim 4\%$. The resources in the case of the 23-qubit code is obtained by replacing 7 with 23 in Eqs. (5.12), (5.13), (5.15), (5.16), (5.20) and (5.21). The

total resources for $p = 3\%$ (4%) amount to $CR \sim 1 \times 10^{25}$ (6×10^{30}) with the help of the resource efficient construction as discussed previously (the standard star-cluster construction results in 10^{40} for $p = 3\%$). The resources are plotted as a function of p for the 23-qubit code (light blue $\times$) in Fig. 5.3.

5.6.3 Small QEC code for an efficient resources usage

We may also consider the four-qubit error-detection code [20]. In this case, the detected errors $\sim p$, which cannot be corrected, are treated as loss errors, and the conditional errors are reduced to $\sim p^2$. Recently, robustness of the surface code under such a noise model has been reported [97, 98, 99]. Specifically with $p = 1\%$, the detected and conditional error probabilities for each root qubit are calculated as 12% and 0.47%, respectively, which seem to be fairly below the threshold [97, 98, 99]. The resources per single logical gate with $p = 1\%$ amount to 3×10^{10}, which is a few order smaller than those for the DV 7-qubit case in Fig. 5.3. However, with $p = 2\%$ the detected and conditional errors are given as 24% and 1.9%, respectively, which would be outside of the correctable region [97, 98, 99].

5.6.4 Perspective for the limitation of the noise threshold

We finally discuss the limitation of the noise threshold at any expense of computational resources (but still polynomial). The perspective is based on the following observations:

(i) Entanglement purification can work even with $p = 10\%$ for the seven-qubit code state.

(ii) The threshold of the entanglement purification increases with the number of qubits in the entangled state (two-colorable graph state), and saturates around 10%, as shown in Fig. 5.4 (a).

(iii) The homogeneous error probabilities $\epsilon_{X,Y,Z}$ of the output state are improved with increasing the number of physical qubits, as shown in Fig. 5.4 (b). This is because a larger entangled state has more stabilizer operators to check.

The above facts (i)–(iii) lead to an expectation that the concatenated seven-qubit code state could be purified even for $p = 10\%$ with a highly homogeneous error distribution in the output state. The correctable error probability of the concatenated seven-qubit code is

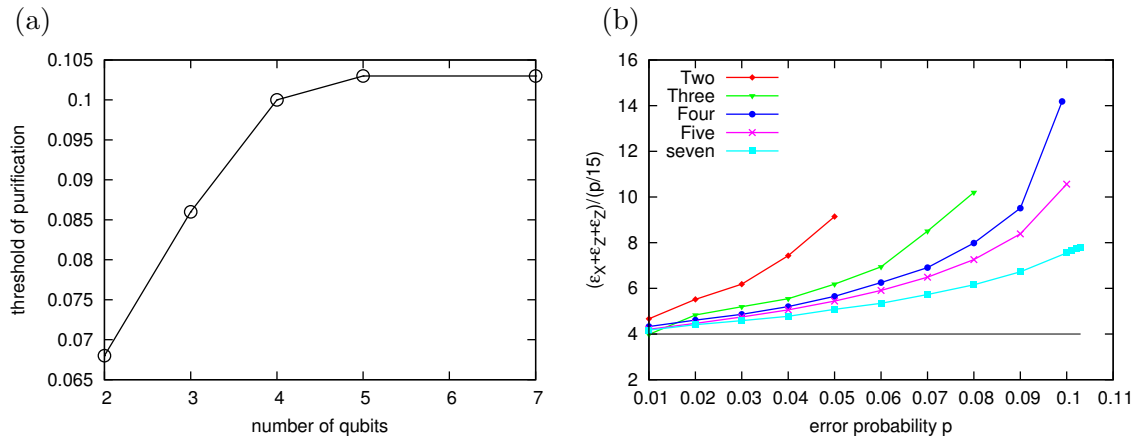


Figure 5.4: (a) The noise threshold of entanglement purification is plotted as a function of the number of qubits in the cluster state. (b) The total output error probability $(\epsilon_X + \epsilon_Y + \epsilon_Z)/(p/15)$ is plotted as a function of the physical error probability p for each two- (red $\Diamond$), three- (green $\triangledown$), four- (blue $\bigcirc$), five- (purple $\times$), and seven-qubit (light blue $\square$) cluster states.

11% with adoptive decoding [110, 111], which is well above the physical error probability $p^{(0)} = 4.7\%$ [see Eq. (5.4)] with $p = 10\%$. Thus for a sufficiently high concatenation level, the logical error probability becomes smaller than the threshold value of the surface code, and the TOWC can be performed reliably. The resources for the star cluster would be extremely huge but still a constant overhead, ensuring that the total resources are polynomial. This concludes the noise threshold of the fault-tolerant TOWC on the 3D cluster state of logical qubits would be significantly high $\sim 10\%$ potentially.

On the other hand, it would be hopeless to improve the noise threshold far above 10%. This is because, as noted in Chapter 4, the noise threshold of entanglement purification with double selection is very close to the upper bound derived in Ref. [125], and the noise threshold of fault-tolerant computation is also subject to the bound. Furthermore, the upper bound of the noise threshold for fault-tolerance has been also obtained as 13.7% by considering the limitation of the magic state distillation [129]. These evidences indicate that the real noise threshold of fault-tolerant quantum computation with a polynomial overhead would be posted around 10%.

5.7 Conclusion

We have investigated the fault-tolerant TOWC on the verified logical cluster states. The finite-size cluster states of logical qubits are prepared with postselection. The 3D cluster

state for TOWC is constructed from them near-deterministically. The present scheme works with a significantly high error rate 2 %, suggesting potentially an even higher noise threshold $5 - 10\%$. The resources usage with $p = 1\%$ are smaller than those for the best known scheme (Knill's error-correcting $C4/C6$ architecture [20]). The resources usages for $p = 3, 4\%$ are also obtained within a reasonable level. We have also mentioned the perspective for the limitation of the noise threshold. The real noise threshold with a polynomial overhead would exist around $p = 10\%$.

Chapter 6

Summary and conclusions

We have investigated fault-tolerant quantum computation on logical cluster states. Computational resource states are prepared offline in the cluster model. This enable us to prepare the cluster states of logical qubits with significantly high fidelity, which leads to a high noise threshold under a reasonable overhead.

We have first investigated an efficient architecture for fault-tolerant quantum computation, which is based on the cluster model of logical qubits. Some relevant logical cluster states, fundamental clusters, are constructed through verification in concatenation, which provides the error-precorrection of gate operations for the one-way computation at the higher level. A suitable code such as the Steane seven-qubit code is adopted for transversal operations. This construction of fundamental clusters provides a simple transversal structure of logical errors in concatenation, and achieves a high noise threshold by using appropriate verification protocols, namely the single and double verifications. Since the postselection is localized within each fundamental cluster with the help of deterministic bare CZ gates without verification, divergence of resources is restrained, which reconciles postselection with scalability. Detailed numerical simulations have really confirmed these desired features of the cluster-based architecture. Specifically, the noise threshold is estimated to be about 3%, and the resources usage are much less than those of the usual circuit-based QEC schemes with the Steane seven-qubit code. This performance is comparable to that of the error-correcting C_4/C_6 architecture with the Fibonacci scheme.

We have then investigated entanglement purification with double selection under imperfect local operations. It has been shown that the double-selection protocol improves significantly the purification performance compared with the usual protocol with single selection. That is, the double-selection protocol has higher noise thresholds for the local

operations and communication channels, and achieves higher fidelity of purified states. It also provides a reasonable yield comparable to or even better than that of the single selection. It has been shown that the purification fidelity is limited by the intrinsically undetectable errors which are introduced by the final gate operations. The double selection is a simple method to remove certainly all the detectable errors in the first order so that it achieves the upper bound on the fidelity in the low noise regime. The double selection has been further applied to the purification of multi-partite entanglement, specifically two-colorable graph states. The improvement of the fidelity and noise threshold has been shown for the Steane seven-qubit code state as a typical example. The double selection can be extended for various graph states in the same way. These results really indicate that the double selection is profitable for entanglement-based protocols. Since multi-partite entangled states, such as CSS codes and cluster states, play important roles in quantum computation as well as quantum communication, the double selection has a good potential to improve the performance of quantum computation.

Finally we have investigated fault-tolerant topological one-way computation on verified logical cluster states. The finite-size cluster states, star clusters, are prepared with postselection. Then, the 3D cluster state for topological one-way computation is constructed from star clusters near-deterministically. This scheme works with a significantly high error rate $p = 2$ %, suggesting potentially an even higher noise threshold $5 - 10\%$. The resources usage with $p = 1\%$ is much smaller than that of the best known scheme (Knill's error-correcting $C4/C6$ architecture [20]). The resources usage is still moderate for $p = 4\%$ with the 23-qubit code. We have further made the perspective for the limitation of the noise threshold. The real noise threshold with a polynomial overhead would be about $p = 10\%$.

These results really indicate that the present approach, i.e., one-way computation with logical qubits, is very promising for realization of fault-tolerant quantum computation, though it still requires hard experimental efforts to satisfy the fault-tolerance condition. To this end, bottom-up approaches, which make use of the properties of individual physical systems [68, 69, 70, 71, 72, 73, 74, 75, 76], should be further developed. Recently quantum coherence has been paid much attention experimentally and theoretically in biological systems [130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140]. Life is warm and wet, and had been thought so far to have little to do with quantum coherence. We hope that some essential ingredients for realization of quantum computer might be found in the complex

biological systems.

Acknowledgments

First of all, I would like to thank Prof. Katsuji Yamamoto, Prof. Atsushi Fukuyama and Prof. Masao Kitano for their valuable advice on this thesis. I would like to thank my advisor, Prof. Katsuji Yamamoto for his support, guidance, and patience with my poorly written manuscripts, throughout my years since I was an undergraduate student. Anyone who can put up with such a pig-headed advisee like me deserve a medal.

I would like to express my thanks to all the members of the quantum physics group of Department of Nuclear Engineering at Kyoto University for valuable discussions and hospitality. I especially wish to thank Toru Kawakubo for listening to my crazy ideas and providing insightful feedbacks.

My graduate career was supported by Research Fellowships of the Japan Society for the Promotion of Science for Young Scientists under Grant No. 20.2157.

I wish to thank my parents and sister, Hidekazu Fujii, Hiroko Fujii and Yumi Fujii for their unfailing support for a long time. Finally I would like to thank my wife, Rie Fujii for supporting and encouraging me in various respects.

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[2] R. P. Feynman, Int. J. Phys. **21**, 467 (1982).

[3] D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985).

[4] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994) p. 124.

[5] P. W. Shor, SIAM J. of Computing **26**, 1484 (1997).

[6] C. H. Bennett and G. Brassard, in *Proceedings of IEEE Int. Conference on Computers, Systems and Singnal Processing* (IEEE, New York, 1984).

[7] W. K. Wooters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[8] R. Landauer, Philos. Trans. Roy. Soc. London Ser. A **353**, 367 (1995).

[9] W. H. Zurek, Rev. Mod. Phys. **75**, 715 (2003).

[10] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

[11] P. W. Shor, "*Proceedings of the 37th Annual Symposium on Foundations of Computer Science*," (IEEE Computer Society Press, Los Alamitos, CA, 1996) p. 56.

[12] D. P. DiVincenzo and P. W. Shor, Phys. Rev. Lett. **77**, 3260 (1996).

[13] A. Y. Kitaev, Russ. Math. Surv. **52**, 1191 (1997).

[14] J. Preskill, Proc. R. Soc. London A **454**, 385 (1998).

[15] E. Knill, R. Laflamme, and W. H. Zurek, Proc. R. Soc. London A **454**, 365 (1998).

[16] E. Knill, R. Laflamme, and W. H. Zurek, Science **279**, 342 (1998).

[17] D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation* (ACM Press, NY, 1998) p. 176.

[18] D. Aharonov and M. Ben-Or, SIAM J. Compt. **38**, 1207 (2008).

[19] A. M. Steane, Phys. Rev. A **68**, 042322 (2003).

[20] E. Knill, Nature (London) **434**, 39 (2005).

[21] P. Aliferis, D. Gottesman, and J. Preskill, Quant. Inf. Comput. **6**, 97 (2006).

[22] P. Aliferis and A. W. Cross, Phys. Rev. Lett. **98**, 220502 (2007).

[23] P. Aliferis, D. Gottesman, and J. Preskill, Quant. Inf. Comput. **8**, 181 (2008).

[24] P. Aliferis and J. Preskill, Phys. Rev. A **79**, 012332 (2009).

[25] K. Fujii and K. Yamamoto, Phys. Rev. A **81**, 042324 (2010).

[26] K. Fujii and K. Yamamoto, arXiv:1008.2048(2010).

[27] B. Eastin, Phys. Rev. A **75**, 022301 (2007).

[28] K. Fujii and K. Yamamoto, in *Proceedings of the 8th International Conference of QCMC* (NICT Press, Tokyo, 2007) p. 105.

[29] K. Fujii and K. Yamamoto, in *Proceedings of the 9th International Conference of QCMC* (AIP Press, Melville, NY, 2009) p. 141.

[30] K. Fujii and K. Yamamoto, Phys. Rev. A **80**, 042308 (2009).

[31] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).

[32] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

[33] E. Bernstein and U. Vazirani, SIAM J. of Computing **26**, 1411 (1997).

[34] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[35] D. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989) p. 69.

[36] D. Gottesman, Ph.D. thesis, California Institute of Technology (1997).

[37] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[38] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).

[39] X. Zhou, D. W. Leung, and I. L. Chuang, Phys. Rev. A **62**, 052316 (2000).

[40] N. Yoran and B. Reznik, Phys. Rev. Lett. **91**, 037903 (2003).

[41] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[42] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).

[43] M. A. Nielsen, Rep. Math. Phys. **57**, 147 (2006).

[44] H.-J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).

[45] K. Chen and H.-K. Lo, Quant. Inf. Comp. **7**, 689 (2007).

[46] M. V. Nest, J. Dehaene, and B. D. Moor, Phys. Rev. A **69**, 022316 (2004).

[47] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. V. Nest, and H.-J. Briegel, *Quantum computers, algorithms and chaos, International School of Physics Enrico Fermi*, Vol. 162 (IOS Press, Amsterdam, 2006).

[48] E. Knill, R.Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).

[49] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).

[50] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).

[51] L.-M. Duan and R. Raussendorf, Phys. Rev. Lett. **95**, 080503 (2005).

[52] S. D. Barrett and P. Kok, Phys. Rev. A **71**, 060310(R) (2005).

[53] Q. Chena, J. Cheng, K.-L. Wang, and J. Du, Phys. Rev. A **73**, 012303 (2006).

[54] D. Gross, K. Kieling, and J. Eisert, Phys. Rev. A **74**, 042343 (2006).

[55] P. P. Rohde and S. D. Barrett, New J. Phys. **9**, 198 (2007).

[56] K. Kieling, D. Gross, and J. Eisert, New J. Phys. **9**, 200 (2007).

[57] Y. Matsuzaki, S. C. Benjamin, and J. Fitzsimons, Phys. Rev. Lett. **104**, 050501 (2010).

[58] R. Raussendorf, Ph.D. thesis, Ludwig-Maximillians Universität München (2003).

[59] M. A. Nielsen and C. M. Dawson, Phys. Rev. A **71**, 042323 (2005).

[60] P. Aliferis and D. W. Leung, Phys. Rev. A **73**, 032308 (2006).

[61] C. M. Dawson, H. L. Haselgrove, and M. A. Nielsen, Phys. Rev. Lett. **96**, 020501 (2006).

[62] C. M. Dawson, H. L. Haselgrove, and M. A. Nielsen, Phys. Rev. A **73**, 052306 (2006).

[63] J. .Cho, Phys. Rev. A **76**, 042311 (2007).

[64] H. Breuer and F. Petruccione, *The Theory of Open Quantum Systems* (Oxford University Press, Oxford, 2002).

[65] H. J. Briegel and B. G. Englert, Phys. Rev. A **47**, 3311 (1993).

[66] W. Dür, J. I. C. M. Hein, and H.-J. Briegel, Phys. Rev. A **72**, 052326 (2005).

[67] H. K. Ng and J. Preskill, Phys. Rev. A **79**, 032318 (2009).

[68] W. Zurek, Phys. Rev. Lett. **53**, 391 (1984).

[69] L. Vaidman, L. Goldenberg, and S. Wiesner, Phys. Rev. A **54**, 1745 (1996).

[70] L. M. Duan and G. C. Guo, Phys. Rev. A **57**, 2399 (1998).

[71] L. Viola and S. Lloyd, Phys. Rev. A **58**, 2733 (1998).

[72] L. Viola, Phys. Rev. A, 012307(2002).

[73] P. Facchi, S. Tasaki, S. Pascazio, H. Nakazato, A. Tokuse, and D. A. Lidar, Phys. Rev. A **71**, 022302 (2005).

[74] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

[75] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **79**, 1953 (1997).

[76] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).

[77] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[78] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).

[79] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[80] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[81] D. Gottesman, Phys. Rev. A **57**, 127 (1998).

[82] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).

[83] A. M. Steane, Phys. Rev. Lett. **78**, 2252 (1997).

[84] D. P. DiVincenzo and P. Aliferis, Phys. Rev. Lett. **98**, 020501 (2007).

[85] M. B. Plenio, V. Vedral, and P. L. Knight, Phys. Rev. A **55**, 4593 (1997).

[86] W. Dür, H. Aschauer, and H. J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).

[87] H. Aschauer, W. Dür, and H. J. Briegel, Phys. Rev. A **71**, 012319 (2005).

[88] A. M. Steane, Nature (London) **399**, 124 (1999).

[89] A. W. Cross, D. P. DiVincenzo, and B. M. Terhal, arXiv:0711.1556(2007).

[90] A. Y. Kitaev, quant-ph/9707021(1997).

[91] E. Dennis, A. Y. Kitaev, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).

[92] R. Raussendorf, J. Harrington, and K. Goyal, Ann. Phys. **321**, 2242 (2006).

[93] R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).

[94] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007).

[95] A. G. Fowler, A. M. Stephens, and P. Groszkowski, Phys. Rev. A **80**, 052312 (2009).

[96] R. Raussendorf, S. Bravyi, and J. Harrington, Phys. Rev. A **71**, 062313 (2005).

[97] T. M. Stace, S. D. Barrett, and A. C. Doherty, Phys. Rev. Lett. **102**, 200501 (2009).

[98] T. M. Stace and S. D. Barrett, Phys. Rev. A **81**, 022317 (2010).

[99] S. D. Barrett and T. M. Stace, arXiv: 1005.2456(2010).

[100] A. M. Steane, Fortschr. Phys. **46**, 443 (1998).

[101] M. A. Nielsen, Phys. Lett. A **308**, 96 (2003).

[102] M. S. Tame, M. Paternostro, and M. S. Kim, New J. Phys. **9**, 201 (2007).

[103] R. Prevedel, M. S. Tame, A. Stefanov, and A. Z. M. Paternostro, M. S. Kim, Phys. Rev. Lett. **99**, 250503 (2007).

[104] E. Knill, Phys. Rev. A **71**, 042322 (2005).

[105] M. Silva, V. Danos, E. Kashefi, and H. Ollivier, New J. Phys. **9**, 192 (2007).

[106] J. Joo and D. L. Feder, Phys. Rev. A **80**, 032312 (2009).

[107] B. W. Reichardt, quant-ph/0406025(2004).

[108] B. W. Reichardt, Quant. Inf. Proc. **4**, 251 (2005).

[109] K. Goyal, A. McCauley, and R. Raussendorf, Phys. Rev. A **74**, 032318 (2006).

[110] D. Poulin, Phys. Rev. A **74**, 052333 (2006).

[111] J. Fern, Phys. Rev. A **77**, R010301 (2008).

[112] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[113] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[114] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[115] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[116] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[117] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[118] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, R4075 (1998).

[119] K. Goyal, A. McCauley, and R. Raussendorf, Phys. Rev. A **74**, 032318 (2006).

[120] S. Glancy, E. Knill, and H. M. Vasconcelos, Phys. Rev. A **74**, 032319 (2006).

[121] C. Kruszynska, A. Miyake, H.-J. Briegel, and W. Dür, Phys. Rev. A **74**, 052316 (2006).

[122] C. Kruszynska, S. Anders, W. Dür, and H.-J. Briegel, Phys. Rev. A **73**, 062328 (2006).

[123] A. Miyake and H.-J. Briegel, Phys. Rev. Lett. **95**, 220501 (2005).

[124] E. N. Maneva and J. A. Smolin, "Quantum computation and quantum information," (American Mathemathical Society, Providence, RI, 2002).

[125] A. Kay, Phys. Rev. A **77**, 052319 (2008).

[126] W. Dür and H.-J. Briegel, Rep. Prog. Phys. **70**, 1381 (2007).

[127] C. Wang, J. Harrington, and J. Preskill, Ann. Phys. **303**, 31 (2003).

[128] T. Ohno, G. Arakawa, I. Ichinose, and T. Matsui, Nuc. Phys. B **697**, 462 (2004).

[129] M. B. Plenio and S. Virmani, New J. Phys. **12**, 033012 (2010).

[130] G. S. Engel, T. R. Calhoun, E. L. Read, T.-K. Ahn, T. Mančal, Y.-C. Cheng, R. E. Blankenship, and G. R. Fleming, Nature (London) **446**, 782 (2007).

[131] H. Lee, Y.-C. Cheng, and G. R. Fleming, Science **316**, 1462 (2007).

[132] E. Collini, C. Y. Wong, K. E. Wilk, P. M. G. Curmi, P. Brumer, and G. D. Scholes, Nature (London) **463**, 644 (2010).

[133] G. Panitchayangkoon, D. Hayes, K. A. Fransted, J. R. Caram, E. Harel, J. Wen, R. E. Blankenship, and G. S. Engel, PNAS **107**, 12766 (2010).

[134] P. Rebentrost, M. Mohseni, I. Kassal, S. Lloyd, and A. Aspuru-Guzik, New J. Phys. **11**, 033003 (2009).

[135] M. B. Plenio and S. F. Huelga, New J. Phys. **10**, 113019 (2008).

[136] M. Sarovar, A. Ishizaki, G. R. Fleming, and K. B. Whaley, Nat. Phys. **6**, 462 (2010).

[137] I. K. Kominis, Phys. Rev. E **80**, 056115 (2009).

[138] J. Cai, G. G. Guerreschi, and H.-J. Briegel, Phys. Rev. Lett. **104**, 220502 (2010).

[139] E. Gauger, E. Rieper, J. J. L. Morton, S. C. Benjamin, and V. Vedral, arXiv: 0906.3725(2009).

[140] K. Fujii and K. Yamamoto, Phys. Rev. A **82**, 042109 (2010).